

AMC/HIPAA Workgroup

Guidelines for Academic Medical Centers on Security and Privacy

*Practical Strategies for Addressing the Health
Insurance Portability and Accountability Act*

May 2001

Version 1.0

Based on

**HIPAA Security and Electronic Signature
Standards; Proposed Rule 8/12/1998**

and

**HIPAA Standards for Privacy of Individually
Identifiable Health Information; Final Rule 12/28/2000**

AMC/HIPAA Workgroup

Abstract

Most health care organizations are now actively interested in implementing the security and privacy measures called for by the HIPAA regulations and are wondering how to get started with this complex, long-lived, and expensive task. This document was developed to help Academic Medical Centers address the HIPAA security and privacy regulations. As we developed this document, we identified a number of key factors that will facilitate HIPAA compliance work. These include:

Awareness: Create and run awareness sessions.

Awareness is important at all levels of the organization, but at the early stages it is most essential for middle and upper management. HIPAA planning cannot move forward in any substantial way until the stakeholders of the organization are actively engaged in creating plans and organizational approaches and developing cost estimates.

Start Correctly and Early: HIPAA is a compliance issue; treat it as one.

It is important for everyone, especially senior managers, to understand that HIPAA is a regulatory compliance project rather than simply an IT initiative. Treating it as a compliance issue is much more likely to lead to the appropriate organization, attention level, and allocation of resources. Resources need to be in the budget cycle for the upcoming fiscal year in order to meet the aggressive timeline.

Standardize your Approach:

Many of the security and privacy requirements can best be met by creating guidelines, principles, templates, and checklists that are then used consistently in each domain (e.g., system, department, division). This will save staff time by creating an efficient, consistent approach. Consistency will make the system more understandable to those who work across various domains and will make the approach more defensible to those with oversight roles (e.g., risk managers, external auditors, JCAHO).

Success Requires Cultural Change:

To run a successful HIPAA-compliant operation, most organizations will have to go through a cultural change in how they manage privacy and security until the new methods become systematic and reflexive. Responses that are not common now will need to become so for a large percentage of the workforce. Many of the HIPAA requirements point up the need for this kind of “new common sense.” Widespread cultural change requires commitment and leadership across an organization.

HIPAA Will Endure:

HIPAA, and the good privacy and security practices it mandates, will require ongoing effort and commitment. These activities must become part of an organization’s ongoing operations and culture.

HIPAA is an Asset:

Increasingly, the public has significant and pervasive concerns about privacy and confidentiality in the electronic world. This is especially true where protected health information is involved.

AMC/HIPAA Workgroup

AMCs that implement appropriate and comprehensive security and privacy policies will build and maintain confidence in their enterprises. Demonstrating a commitment to protect security and privacy will help build patient loyalty and support the research and clinical enterprise.

Executive Summary

The HIPAA security and privacy regulations exist for good reasons

Storing and transmitting health information in electronic form exposes it to risks that do not exist, or exist to a lesser degree, when it is maintained in paper. Health information is a vital business asset for a healthcare organization, and protecting it preserves the value of this asset. In addition, securing patients' information protects their privacy and enhances the organization's reputation for professionalism and trustworthiness. Healthcare organizations have long recognized the value of health information, and are already taking many of the measures required by the HIPAA security and privacy regulations. Nevertheless, complying with HIPAA will require most covered entities (entities subject to the Security and Privacy regulations) to adopt new policies and procedures for handling protected health information (individually identifiable health information held by a covered entity) and to make some hard choices about how these policies will be implemented. This report offers guidance in making those choices, and discusses good healthcare security and privacy practices.

Covered entities should plan to comply within the next two years

The final HIPAA security and privacy regulations will become effective two years after the date of their publication in the Federal Register.

The final HIPAA security rule has not been published at this time, so its compliance date has not been set. Publication of the final security rule in the Federal Register is anticipated in the third or fourth quarter of 2001; however, covered entities should plan to be in compliance by the middle of 2003.

The final HIPAA privacy rule was published in the Federal Register on December 28, 2000, but its official effective date was moved forward due to administrative issues. The compliance date for large covered entities (such as AMCs) is April 14, 2003.

Many of the regulations' requirements are clear and specific

Although the HIPAA security and privacy regulations are long and complex, many of their requirements are clear and specific. The major actions the regulations require a covered entity to take are:

- ◆ Assign responsibility for security to a person or an organization.
- ◆ Assess risks and determine the major threats to the security and privacy of protected health information.
- ◆ Set up a security management program that addresses physical security, personnel security, technical security controls, security incident response, and disaster recovery.
- ◆ Certify the effectiveness of new or existing security controls.
- ◆ Appoint a privacy officer and a point of contact for receiving privacy complaints.
- ◆ Adopt a privacy policy and publicize the policy by giving notice. Privacy policies must have specific provisions for gaining consent and authorization to use protected health

AMC/HIPAA Workgroup

information, restricting use and disclosure of protected health information, and receiving and resolving complaints.

- ◆ Change contracts and business partner agreements to include a contractual requirement that partners handle protected health information properly.
- ◆ Train the covered entity's workforce (and business associates who work on the covered entity's premises) to follow proper security and privacy policies and procedures.
- ◆ Document security and privacy policies and procedures, as well as actions taken to ensure that policies and procedures are enforced.

This document explains these requirements in more detail and gives specific recommendations on how Academic Medical Centers can implement them.

Some of the regulations' provisions require covered entities to exercise judgment

While many of the provisions of the HIPAA security and privacy regulations require little interpretation, some deliberately provide room for interpretation to allow covered entities the flexibility they need to comply without making unnecessarily disruptive changes. This document points out which of the regulations' requirements a covered entity will have to interpret, and provides guidance on some of the options Academic Medical Centers should consider. Topics addressed include:

- ◆ **Assignment of responsibilities.** The regulations require covered entities to assign specific responsibilities. These requirements could be handled by creating new executive positions or departments, or they could be handled by allocating new responsibilities to existing positions and departments. This document discusses how to assign responsibilities in the context of your existing organizational structure, and includes sample job descriptions for some of the required positions.
- ◆ **Defining and introducing policies.** A broad range of security and privacy policies and procedures could be used to safeguard protected health information. This document discusses processes for defining and introducing policies and procedures that will be effective in your organization. Sample security and privacy policies are included.
- ◆ **Risk analysis.** The regulations require covered entities to analyze risks to security and privacy of health information, and to determine whether the risks are "acceptable." This document discusses how to choose a risk analysis methodology and how to decide what constitutes "acceptable risk," and gives references to several risk analysis methodologies.
- ◆ **Certification.** The regulation requires covered entities to certify security controls. An internal organization or a third party can perform the required certification, and the regulation does not mandate a specific certification process or regime. This report discusses some of the certification options.
- ◆ **Scalability.** The regulations allow a covered entity to consider "scalability" (in other words, the cost burden of implementation) when deciding how to implement certain provisions. This document addresses "scalability" issues.
- ◆ **Minimum necessary information.** The privacy regulation requires covered entities to restrict use and disclosures of private information to "the minimum use or disclosure necessary to accomplish the purpose of the request." This document discusses how to determine what information is necessary in a given situation.

AMC/HIPAA Workgroup

- ◆ **Managing consumer requests.** The privacy regulation requires covered entities to implement a process for receiving and responding to complaints, as well as to requests to restrict access to information. This document discusses some of the options for managing these complaints and requests.
- ◆ **Contracts.** The regulations require that security and privacy provisions be incorporated into contracts with other organizations. This document discusses options for doing so and includes some model contract terms.
- ◆ **Disclosure.** The privacy regulation offers several options relating to the disclosure and use of de-identified information. This document addresses how to choose an option.

Key activities for HIPAA security and privacy compliance

In addition to providing information about how to handle specific aspects of HIPAA security and privacy compliance, this document outlines a framework for addressing the regulations. The framework includes the following sequence of activities:

- 1) Recognize that HIPAA security and privacy compliance is a policy and compliance effort, not a technology effort.
- 2) Assign responsibility for HIPAA compliance.
- 3) Consult widely with stakeholders.
- 4) Formulate job descriptions for the officials required by the HIPAA regulations (security and privacy officials, complaint receivers).
- 5) Hire or appoint the required officials.
- 6) Perform an initial risk analysis, including an asset inventory.
- 7) Review the results of the risk analysis with senior management.
- 8) Create a HIPAA security and privacy compliance program. A compliance program must include written policies and procedures, a compliance office reporting to senior executive management, compliance training, a complaint process, an internal compliance audit program, sanctions, and incident response and corrective action procedures.
- 9) Formulate or update security and privacy policies.
- 10) Update the risk analysis based on the new policies.
- 11) Create a detailed HIPAA security and privacy compliance plan, including security and privacy procedures, security and privacy training, security and privacy evaluation and certification, and disaster recovery procedures. This report suggests establishing a formal security management program as part of the HIPAA security and privacy compliance plan.
- 12) Review the compliance plan with senior management.
- 13) Execute the compliance plan (in phases if appropriate).
- 14) Document the compliance plan and its execution.
- 15) Operate the compliance plan and the security management program on a continuing basis. Include regular reports to senior management. Update the risk analysis regularly.

Detailed advice on topics that organizations should consider as they perform these activities is provided throughout the report.

Many will face serious organizational issues on the way to compliance

AMC/HIPAA Workgroup

Compliance with the HIPAA security and privacy regulations will raise a variety of issues. This report describes some of the issues Academic Medical Centers are most likely to encounter, and provides some options for dealing with these issues. Specifically, this report addresses:

- ◆ **Organizational structure.** Academic Medical Centers typically have a complex organizational structure, with many sub-entities and affiliates in a complicated governance arrangement. This report discusses which entities are covered by the HIPAA security and privacy regulations and how a covered entity's structure influences the activities required to bring it into compliance.
- ◆ **Changing practices.** Some HIPAA security and privacy compliance activities require changing established patterns of thought and behavior. Healthcare workers use protected health information in their day-to-day job activities. Some information use practices will have to change in order to comply with the HIPAA security and privacy regulations' requirements. This report discusses how a covered entity can introduce changes in long-established information and system use practices by building awareness and encouraging buy-in.
- ◆ **Financial.** Compliance activities cost money. This report discusses approaches to funding compliance activities.
- ◆ **Locating resources.** Many healthcare organizations lack security and privacy expertise. This report discusses where to find information about security and privacy.
- ◆ **Interpretation.** As already discussed, the HIPAA security and privacy regulations leave room for interpretation in many areas. This report addresses how to interpret the regulations' gray areas.
- ◆ **Research and education.** The HIPAA security and privacy regulations have special provisions for research and educational uses of protected health information. This report addresses how an Academic Medical Center's research and education activities will be affected by the regulations.
- ◆ **Fundraising and marketing.** The HIPAA security and privacy regulations have provisions relating to fundraising and marketing activities. This report addresses how an Academic Medical Center's fundraising and marketing will be affected by the regulations.

Compliance will carry significant costs, but it will also bring benefits

Complying with the HIPAA security and privacy regulations will require new policies, procedures, and processes. It will increase the paperwork associated with disclosing protected health information. It will also require new training and certification activities. None of this comes for free.

The money and effort spent to comply with the HIPAA security and privacy regulations will, however, buy significant benefits for the organization even above and beyond avoiding penalties for non-compliance. Compliance with HIPAA security and privacy standards will play an important role in preserving patients' trust in the healthcare system, the organization, and individual healthcare providers. HIPAA security and privacy compliance can help healthcare organizations avoid the adverse publicity and public image problems which disclosures of

AMC/HIPAA Workgroup

personal information have inflicted on web retailers recently. Covered entities should view security and privacy as yet another benefit they can offer to patients who choose their services.

Compliance with the HIPAA security regulation can also reduce a covered entity's business risks significantly. A strong security management program reduces the probability of interruption of business, destruction of the organization's information assets, and damage to brand and reputation due to vandalism of information systems. Compliance may also shield covered entities from significant fines, loss of accreditation, and loss of consumer trust. Finally, it can reduce exposure to liabilities associated with improper handling of protected health information.

AMC/HIPAA Workgroup

Contents

Abstract	ii
Executive Summary	iv
Contents.....	ix
Introduction	1
Purpose.....	2
Scope	2
Background	3
Acknowledgements	3
Updates and Errata	6
AMC Guidelines	7
Organization of the Guidelines	7
AMC HIPAA Security Guidelines.....	9
Section One: Requirements for Security Administration.....	9
SEC.01 Certification § .308(a)(1)	10
SEC.02 Chain of Trust Partner Agreement § .308(a)(2).....	12
SEC.03 Contingency Planning § .380 (a)(3).....	14
SEC.04 Formal Mechanism for Processing Records § .308(a)(4)	16
SEC.05 Information Access and Control § .308(a)(5).....	17
SEC.06 Internal Audit § .308(a)(6).....	19
SEC.07 Personnel Security § .308(a)(7)	21
SEC.08 Security Configuration Management § .308(a)(8).....	23
SEC.09 Security Incident Procedures § .308(a)(9)	25
SEC.10 Security Management Process § .308(a)(10).....	27
SEC.11 Termination Procedures § .308(a)(11).....	30
SEC.12 Security Training § .308(a)(12)	32
Section Two: Requirements for Physical Safeguards	35
SEC.13 Assigned Security Responsibility § .308(b)(1).....	36
SEC.14 Media Controls § .308(b)(2)	38
SEC.15 Physical access controls § .308(b)(3).....	41
SEC.16 Policy/guideline on workstation use § .308(b)(4).....	44
SEC.17 Secure work station location § .308(b)(5).....	46
SEC.18 Security Awareness training § .308(b)(6).....	48
Section Three: Requirements for Technical Security, Services, and Mechanisms.....	49
SEC.19 Access Control § .308(c)(1)(i)	50
SEC.20 Audit Controls § .308(c)(1)(ii).....	52
SEC.21 Authorization Control § .308 (c)(3).....	54
SEC.22 Data Authentication § .308 (c)(4)	55
SEC.23 Entity Authentication § .308 (c)(5).....	56
SEC.24 Communications/network controls § .308(d)	58
AMC HIPAA Privacy Guidelines.....	61
Section One: Covered Entities	65
PRIV.01 Health care component §164.504(b).....	66
PRIV.02 Affiliated covered entities §164.504(d)	68
PRIV.03 Business associate contracts §164.504(e)(1).....	70

AMC/HIPAA Workgroup

PRIV.04	Requirements for group health plans §164.504(f)(1).....	74
PRIV.05	Requirements for a covered entity with multiple covered functions § 164.504(g)	78
PRIV.06	Group health plans § 164.530(k).....	80
Section Two: Consent and Authorization		81
PRIV.07	Consent requirement § 164.506(a).....	82
PRIV.08	Resolving conflicting consents and authorizations § 164.506(e).....	86
PRIV.09	Joint consents § 164.506(f)	88
PRIV.10	Authorizations for uses and disclosures § 164.508(a)	90
PRIV.11	Right of an individual to request restriction of uses and disclosures § 164.522(a)(1).....	96
PRIV.12	Effect of prior consents and authorizations § 164.532(a)	98
Section Three: Uses and disclosures		101
Sub-Section A: General Uses and Disclosures		102
PRIV.13	Uses and disclosures of protected health information § 164.502(a)	103
PRIV.14	Uses and disclosures of protected health information subject to an agreed- upon restriction § 164.502(c)	105
PRIV.15	Uses and disclosures of de-identified protected health information § 164.502(d)	107
PRIV.16	Disclosures to business associates § 164.502(e).....	108
PRIV.17	Deceased individuals § 164.502(f).....	110
PRIV.18	Personal representatives § 164.502(g)	111
PRIV.19	Confidential communications § 164.502(h).....	113
PRIV.20	Uses and disclosures consistent with notice § 164.502(i).....	114
PRIV.21	Disclosures by whistleblowers and workforce member crime victims § 164.502(j)	115
PRIV.22	Use and disclosure for facility directories § 164.510(a)	117
PRIV.23	Uses and disclosures for involvement in the individual's care and notification purposes § 164.510(b)	119
PRIV.24	Uses and disclosures of protected health information for marketing § 164.514(e)(1).....	121
PRIV.25	Uses and disclosures for fundraising § 164.514(f)(1).....	123
PRIV.26	Uses and disclosures for underwriting and related purposes § 164.514(g)125	
Sub-Section B: Balancing Privacy and Public Responsibility		126
PRIV.27	Uses and disclosures required by law § 164.512(a).....	127
PRIV.28	Uses and disclosures for public health activities § 164.512(b).....	128
PRIV.29	Disclosures about victims of abuse, neglect, or domestic violence § 164.512(c)	130
PRIV.30	Uses and disclosures for health oversight activities § 164.512(d).....	132
PRIV.31	Disclosures for judicial and administrative proceedings § 164.512(e).....	134
PRIV.32	Disclosures for law enforcement purposes § 164.512(f)	137
PRIV.33	Uses and disclosures about decedents § 164.512(g).....	141
PRIV.34	Uses and disclosures for cadaveric organ, eye, or tissue donation purposes § 164.512(h)	143
PRIV.35	Uses and disclosures for research purposes § 164.512(i)	144

AMC/HIPAA Workgroup

PRIV.36	Uses and disclosures to avert a serious threat to health or safety § 164.512(j)	148
PRIV.37	Uses and disclosures for specialized government functions § 164.512(k)	150
PRIV.38	Disclosures for workers' compensation § 164.512(l)	153
PRIV.39	Minimum necessary § 164.502(b)	154
PRIV.40	De-identification of protected health information § 164.514 (a)	156
PRIV.41	Minimum necessary requirements § 164.514(d)(1)	160
PRIV.42	Verification requirements § 164.514(h)(1)	163
Section Four: Consumer Controls		166
PRIV.43	Notice of privacy practices § 164.520(a)	167
PRIV.44	Confidential communications requirements § 164.522(b)(1)	173
PRIV.45	Access to protected health information § 164.524(a)	175
PRIV.46	Right to amend § 164.526(a)	181
PRIV.47	Right to an accounting of disclosures of protected health information § 164.528(a)	185
Section Five: Administrative requirements		189
PRIV.48	Privacy Official § 164.530(a)(1)(i)	190
PRIV.49	Privacy Contact Person or Office § 164.530(a)(1)(ii)	192
PRIV.50	Training on Privacy § 164.530(b)(1)	194
PRIV.51	Safeguards § 164.530(c)(1)	196
PRIV.52	Complaints to the covered entity § 164.530(d)(1)	198
PRIV.53	Sanctions § 164.530(e)(1)	200
PRIV.54	Mitigation § 164.530(f)	202
PRIV.55	Refraining from intimidating or retaliatory acts § 164.530(g)	204
PRIV.56	Waiver of rights § 164.530(h)	206
PRIV.57	Policies and procedures § 164.530(i)(1)	207
PRIV.58	Changes to policies or procedures § 164.530(i)(2)	208
PRIV.59	Documentation § 164.530(j)	211
General Policy and Management Guidelines		213
GEN.01	Roles and Responsibilities in Development and Maintenance	214
GEN.02	Organizational Support for HIPAA Security and Privacy Compliance	216
GEN.03	Resources for Development and Maintenance	217
GEN.04	Evaluation and Monitoring of Development and Maintenance	218
GEN.05	Reasonableness	219
GEN.06	Scalability	220
GEN.07	Limiting Liability Arising from Compliance	221
GEN.08	HIPAA Accreditation Intersections	222
GEN.09	Stricter State Law § 160.203	223
GEN.10	Policy establishment and modification	225
GEN.11	Policy Usage Introduction	226
GEN.12	Privacy Culture	227
GEN.13	Digital Signature	228
GEN.14	Other Federal Law and HIPAA Privacy	231
Acronyms		234
Definitions of Terms Used in this Guideline		235
References		243

AMC/HIPAA Workgroup

Privacy Standards 245

TABLES

Table 1. Mapping of Privacy Standards to AMC Guidelines 61

AMC/HIPAA Workgroup

Introduction

The privacy and security regulations mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are of great importance to the healthcare community. In an effort to assist Academic Medical Centers in addressing the new regulations, a series of workshops were conducted to analyze current health information security and privacy policies, to make recommendations, and to develop a resource of best practices for healthcare security and privacy. This document, *Guidelines for Academic Medical Centers on Security and Privacy*, is the result of a collaborative effort by multiple teaching hospitals and medical schools to address their unique concerns in this area.

How are Academic Medical Centers different from other health care providers?

The tripartite mission of Academic Medical Centers (AMCs) — education, research, and patient care — distinguishes them from peer institutions which are concerned primarily with patient care. In the past two decades, the ability of AMCs to sustain these multiple missions has been severely tested by changes in health care financing and regulation. Their history, governance, constituency base, and position in society present unique challenges to successfully navigating change. Implementation of the HIPAA security and privacy regulations, too, will face unique barriers. Yet AMCs also have characteristics that give them advantages over other health care provider organizations in this area, and provide an opportunity for AMCs to lead the effort to ensure the privacy, security, and confidentiality of patient information. The following lists summarize these potential barriers and opportunities.

AMCs: Unique Opportunities to Lead HIPAA Compliance

- ◆ Well-educated, hard-working membership;
- ◆ Traditionally innovators in health care;
- ◆ Strong technology and information systems culture;
- ◆ Active role in national health care policy development.

AMCs: Unique Barriers to HIPAA Compliance

- ◆ Complex organizational and governance structure:
 - ▶ Multiple entities with a single name;
 - ▶ Unclear or non-existent reporting lines;
 - ▶ Governed by boards with a variable level of understanding of medical center issues.
- ◆ University affiliation:
 - ▶ Decentralized organization, an inability to act quickly, and decisions by committee;
 - ▶ Academic culture tends to reward individual vs. organizational action;
 - ▶ Non-employee system users (students, trainees);
 - ▶ Often beholden to central university administration, which may have to sign off on some aspects of compliance activities.
- ◆ Multiple missions:
 - ▶ Confusion and disagreement about priorities;
 - ▶ Cross-subsidization of non-profitable missions.

AMC/HIPAA Workgroup

Purpose

These Guidelines provide a tool for developing policies, procedures, and best practices to assist AMCs in efficiently and economically addressing the HIPAA security and privacy regulations. They reference specific HIPAA regulations, provide interpretation, and make recommendations for implementation and maintenance within healthcare organizations.

Scope

The intent of the workshop series was to provide guidance, within the context of the HIPAA regulations, in the development of security and privacy policies and procedures that support all activities of complex academic medical center environments. Depending on organizational structure, this may include healthcare, research, teaching, learning, administration, and associated interactions with external entities.

The results of these workshops will assist like-minded organizations in developing more efficient and inclusive ways of implementing health care security and privacy arrangements. It is intended that these guidelines be considered for adoption by relevant bodies beyond the covered entities themselves. WEDI, as part of their role in advising HHS in matters related to HIPAA, participated in the workshops and will take the final publication into consideration. The combined talent and experience of the workshop participants have permitted the development of a concise set of guidelines consistent with these purposes.

The intent of the workshop series was to provide guidance, within the context of the HIPAA regulations, in the development of security and privacy policies and procedures that support all activities of complex AMC environments. Depending on organizational structure, this may include healthcare, research, teaching, learning, administration, and associated interactions with external entities.

The results of these workshops will assist like-minded organizations in developing more efficient and inclusive ways of implementing health care security and privacy arrangements. The combined talent and experience of the workshop participants has permitted the development of a concise set of guidelines to assist with HIPAA security and privacy regulations.

These guidelines recommend health information security and privacy mechanisms and strategies for operational implementation of the HIPAA requirements. The recommended strategies are intended to facilitate cultural change by building upon existing best practice, and are based upon our common understanding of teaching hospital and medical school processes. This collaborative effort also identifies implementation barriers that must be overcome, in addition to benefits or incentives that may be leveraged to deploy adequate resources within teaching hospitals and medical schools.

This document *does not* provide legal advice. Covered entities must work with their own legal counsels to address appropriate institutional requirements. This document can provide information to legal staff tasked with understanding the implications of the HIPAA regulation on their organization. It may also serve as an aid to understanding the necessary legal actions needed to address accreditation requirements, as well as federal and state legislation, as HIPAA has an impact on many aspects of the organization.

AMC/HIPAA Workgroup

In addition, this document may be of value to other segments of the healthcare industry, particularly consultants, payor organizations, general practitioners, group practices, suppliers, financial organizations, and other organizations that regularly interact with teaching hospitals and medical schools. Understanding the implications of the HIPAA regulations on AMCs will be important to many aspects of the healthcare industry.

Background

Guidelines for Academic Medical Centers on Security and Privacy was developed through a series of monthly workshops involving the collaborative effort of several major academic and healthcare related organizations. Several leading teaching hospitals and medical schools had already developed individual security and privacy policies, as well as strategies to address the impending HIPAA regulations. No process existed, however, to facilitate the benchmarking of good practices, policies, and procedures among institutions. Academic Medical Centers needed to join together and identify consistencies for reasonable HIPAA compliance. Teaching hospitals and medical schools indicated their willingness and commitment to participate in this process by submitting a Request for Information (RFI) that was developed by the steering committee for this activity.

Information was gathered on current security and privacy practices via responses to the RFI. This information, in addition to the HIPAA regulation, served as the basis for the initial draft. Finally, individuals with substantial expertise were identified and asked to contribute to the effort.

In addition to the teaching hospitals and medical schools, a number of industry organizations joined the group. A series of workshops was identified as the best mechanism to create model information practices and security guidelines, with a final document (this document) to communicate the group's recommendations.

The workshops were held from Fall 2000 to Spring 2001. On December 20, 2000, the Department of Health and Human Services Privacy Regulations were released. When the group first met and planned its workshops, it was impossible to determine when the draft privacy regulation would be made final, and how the final regulation might differ from the draft. Shortly before the fourth workshop, the final privacy regulation was issued. The group opted to hold an additional session to address any modifications to the guidelines as a result of the final privacy regulation.

Acknowledgements

This guideline document is the result of many individuals, those who participated in the workshops and others who helped to facilitate the process to make this document possible. A group with diverse expertise in security and privacy found their way through a consensus based process to produce these guidelines. Each participant in the workshops is commended for their tireless devotion of time and enthusiasm.

AMC/HIPAA Workgroup

Special thanks are due to the organizations that hosted the workshops: Kaiser-Permanente, Duke University, Texas A&M University, the National Library of Medicine, and the University of Michigan. To all the individuals who coordinated the workshop logistics at each of the host organizations, the participants in the workshops extend a thank you for creating extremely productive working environments for this activity.

Thanks to the numerous individuals at each of the participating organizations who helped to provide participants with input and content and kept the workshop participants on track, helping its members to put their ideas and analyses into coherent prose. The workgroup is further indebted to early reviewers of the draft guideline document. Thoughtful comments and criticisms challenged members to strengthen and refine the guidelines.

Mike Ackerman, assistant director of the High Performance Computing Center at the NLM, understood the need for this group to assemble. His support, dedication, and understanding made this report a reality. Thanks to Morgan Passiment and the AAMC staff who provided much time and attention to facilitating the production of the guidelines. Thanks also to Jim Schuping at WEDI for help in getting the first set of interested parties together.

The guideline document is a much more readable document due to the efforts of Joseph Saul of Communications Technology Consultancy, a security and privacy policy expert, who edited the final version. Special thanks are due to Mike Davis for editorial leadership that kept everyone organized and ensured that all input was incorporated into the final guidelines. Thanks are also due to Bob Blakely, OMG, for his dedication to improving security and privacy practices. Bob's enthusiasm, quick wit, and expert technical facilitation kept things on track, allowing discussions to unfold when appropriate, and shutting us down when we needed to stop. Finally, Mary Kratz and the Internet2 staff deserve praise for the great resources that they brought to this project.

The workgroup hopes that this guideline document will assist others in the healthcare industry struggling with practical strategies for dealing with security and privacy issues and HIPAA compliance.

Workshop Participants (alphabetical order by organization)

Duke University Health System Dave Kirby* Director of the Information Security Office 919-272-1157 Kirby001@mc.duke.edu	Duke University Health System Lawrence H. Muhlbauer Assistant Research Professor Lawrence.muhlbauer@duke.edu	Emory University Ron Palmich 404-727-4350 ron_palmich@emory.org
Johns Hopkins Medical Institutions Bob Miller* Department of Pathology 410-955-5429 rmiller@jhmi.edu	Johns Hopkins Medical Bill Rider* brider@jhmi.edu	Kaiser Permanente Ted Cooper* 510-267-5659 ted.cooper@kp.org
Mayo Clinic Lee Olson* Information Security Officer 507-284-0594 olson.lee@mayo.edu	Oregon Health Sciences University Jere Retzer* Portland Research and Education Network Chair Internet2 Health Sciences Security Lead 503-494-3720 retzerj@ohsu.edu	Osaka Medical College Ryuichi Yamamoto Associate Professor Division of Medical Informatics +81-726-83-1221(x2265/2888) yamamoto@art.osaka-med.ac.jp

AMC/HIPAA Workgroup

<p>Texas A&M University System Health Science Center Larry Flournoy Interim Chief Information Officer 713-677-7434 flournoy@isc.tamu.edu</p>	<p>Texas A&M University Michael W. Buckley Director, Compliance and Administration Office of the Vice President of Research 979-845-8585 mw Buckley@tamu.edu</p>	<p>Tufts School of Medicine Davis Damassa 617-636-6603 david.damassa@tufts.edu</p>
<p>University of Alabama at Birmingham Mike Waldrum* mwaldrum@uabmc.edu</p>	<p>University of Arizona Medical Center Patti Redding HIPAA Compliance and Information Security 520-694-4760 predding@umcaz.edu</p>	<p>University of Michigan Health System Leslie H. Kamil Deputy Compliance Officer and Privacy Officer 734-615-4400 lkamil@med.umich.edu</p>
<p>University of Pennsylvania Mary Alice Annecharico Executive Director, Information Services 215-898-9755 mannecha@mail.upenn.edu</p>	<p>University of Tennessee Health Science Center Jack Buchanan Acting Director, School of Biomedical Engineering Internet2 Medical Middleware Lead Jbuchanan@utmem.edu</p>	<p>North Carolina Healthcare Information and Communications Alliance, Inc. W. Holt Anderson Executive Director 919-558-9258 holt@nchica.org</p>
<p>UT Southwestern Medical Center Valerie D. Meyer Information Resources 214-648-1718 Valerie.meyer@utsouthwestern.edu</p>	<p>Veterans Health Administration Mike Davis (SAIC)* VHA Security Architect mikedatsd@home.com</p>	<p>Yale University School of Medicine Stephen Rimar, MD Medical Director, Yale Medical Group stephen.rimar@yale.edu</p>

Sponsoring Organizations

<p>Association of American Medical Colleges Morgan Passiment* Staff Associate 202-828-0476 mpassiment@aamc.org</p>	<p>The AAMC (Association of American Medical Colleges) Group on Information Resources has identified a need for collaboration in policy development among Academic medical centers and agreed to participate in the development of this policy framework as a key component of its program to support the HIPAA implementation activities of its members.</p>
<p>Internet 2 Mary Kratz* Health Science Initiatives 734-352-7004 mkratz@internet2@edu</p>	<p>These guidelines serve as a basis for Internet2 Medical Middleware requirements, ultimately folding into the larger fabric of advanced services in the emerging common campus middleware infrastructure.</p>
<p>National Library of Medicine Michael J. Ackerman, PhD* Assistant Director 301-402-4100 ackerman@nlm.nih.gov</p>	<p><i>The National Library of Medicine (NLM)</i> views its support for this workshop as part of its mission with the teaching hospital and medical school community. <www.nlm.nih.gov></p>
<p>National Library of Medicine Carol Haberman* 301-435-3267 carol_b_haberman@nih.gov</p>	
<p>Object Management Group Bob Blakley* Chief Scientist for Security, Tivoli Systems Incorporated 512-458-4037 blakley@tivoli.com</p>	<p>The OMG's charter includes the establishment of industry guidelines and specifications to provide a common framework for application development that supports a heterogeneous computing environment across all major hardware platforms and operating systems.</p>

Supporting Organizations

<p>CPRI-HOST Pat Wise* Executive Director pat@digitalwise.com</p>	<p>North Carolina Healthcare Information and Communications Association (NCHICA) Holt Anderson</p>
--	---

AMC/HIPAA Workgroup

	919-558-9258 holt@nchica.org
Health Care Financing Administration Barbara Clark 410-786-9937 bclark@hcfa.gov	Healthcare Computing Strategies, Inc. John Parmigiani Practice Director, Compliance Programs 410-750-2060 jcparmigiani@hcs-is.com
Southeastern University Research Association (SURA) Sue Fratkin* 202-408-7872 sue@sura.org	Workgroup on Electronic Data Interchange (WEDI) Jim Schuping* Executive Vice President 703-391-2716 schups@aol.com

* Denotes members of the Steering Committee

Updates and Errata

For updates and errata, check the www.amc-hipaa.org website.

AMC/HIPAA Workgroup

AMC Guidelines

This document provides a summary of the requirements of the HIPAA security and privacy regulations, with advice to the reader on how to address those requirements. The document's structure has been designed to make it easy to relate the material in this document to the text of the HIPAA security and privacy regulations.

Organization of the Guidelines

The document starts with specific information about addressing the detailed requirements of the HIPAA security and privacy regulations where those regulations are clear and specific. It then moves on to cover areas in which some interpretation of the regulations' requirements is necessary. It concludes with a treatment of broader organizational implications of HIPAA security and privacy compliance; this portion of the document covers issues that the regulations raise but for which they provide neither specific requirements nor clear guidance.

The Security sections discuss provisions of the HIPAA Security Regulations:

Security Section One discusses what a covered entity needs to do to address the security administration requirements.

Security Section Two discusses what a covered entity needs to do to address the technical security services and mechanisms requirements.

The Privacy sections discuss provisions of the HIPAA Privacy Regulations:

Privacy Section One discusses the definition of a covered entity and the application of the regulations to different types of covered entities.

Privacy Section Two discusses consent and authorization requirements.

Privacy Section Three discusses use and disclosure requirements.

Privacy Section Four discusses consumer control requirements.

Privacy Section Five discusses administrative requirements.

The General Section covers areas of the HIPAA regulation that require a covered entity to make judgments about how the regulations' requirements apply to the organization (for example, "minimum necessary disclosure," "scalability," and "reasonableness"). This Section also covers broader organizational implications of compliance with the regulations (for example, how HIPAA compliance might influence the structure of the organization, how HIPAA compliance activities might relate to other similar activities, and what time and resources might be required to achieve and maintain HIPAA compliance).

AMC/HIPAA Workgroup

The Guideline points themselves are organized as follows:

Point Number, Point Name and Citation

X.## Name §Citation

HIPAA Requirement

The full text of the HIPAA requirement, taken directly from the regulation. This may include material from multiple portions of the regulations.

AMC Explanation of HIPAA Requirement

This narrative paragraph summarizes the top features of the requirement as seen from the vantage point of an AMC, concentrating on the significance of the requirements in the AMC environment.

Key Issues

Issues to consider before taking any proposed action.

Category I Guideline—Action must be taken to address these

Actions that are *mandatory* in order to address the HIPAA Security and Privacy regulations. The list includes only those actions that, if not addressed, would place a covered entity in substantial non-compliance with the requirement. Actions included in this item were included only with the unanimous consent of all members of the AMC Security and Privacy Workgroup.

Category II Guideline—Action should be considered to address these

Actions that workgroup participants considered *helpful* in order to address the HIPAA Security and Privacy regulations. Actions in this group are recommended by the AMC Security and Privacy Workgroup but are not direct requirements of HIPAA.

Roadblocks

Any roadblocks to what must or should be done in order to implement the guidelines. The AMC Security and Privacy Workgroup defines roadblocks as difficulties in implementing these guidelines that come after the policy is put in place, e.g. AMC culture, program dollars, people, etc. This definition distinguishes roadblocks from *issues*, which are concerns associated with framing an AMC policy through the application of the guideline (and therefore come before the policy). Funding issues and the problems associated with decentralization in AMCs are universal roadblocks, so they have not been listed for individual guideline points unless there is a specific point to be made.

Comments

Any comments to clarify or explain this point above or relate it to another.

AMC/HIPAA Workgroup

AMC HIPAA Security Guidelines

Section One: Requirements for Security Administration

SEC.01 Certification § .308(a)(1)

HIPAA Requirement

...(The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.)

AMC Explanation of HIPAA Regulation

Certification is the process of determining whether technical security controls are implemented and comply with specified criteria. Each covered entity is required to establish a certification process that demonstrates and documents that its computer systems and networks meet these criteria. Either internal staff or external persons may perform certifications. The process should consider risks identified in the risk assessment process.

Key Issues

- ◆ What systems and services require certification?
- ◆ How often should certification occur?
- ◆ Who or what organization is the certifying authority? Is it internal or external? How will the certifying authority be selected?
- ◆ Do reference documents exist to describe the covered entity's secure configuration of network components, servers, databases, and applications?
- ◆ Is there a periodic comparison of the actual configuration against the reference documents to confirm compliance or reveal non-compliance? If there are differences, is there a process for correction?
- ◆ Do routine testing, auditing, and change management procedures support the certification process?
- ◆ What is the relationship between auditors and certifiers?
- ◆ With what frequency or upon what event(s) should certification be done?

Category I Guidelines-Actions must be taken to address these

- ◆ Implement a certification process to determine the extent to which systems and networks meet established security criteria.

Category II Guidelines-Actions should be taken to address these

- ◆ Document the network configuration.
- ◆ Ensure that individuals performing certifications are knowledgeable about security requirements and best practices.
- ◆ Ensure that conflicts of interest do not exist in the certification process—specifically that certifiers are not responsible for the system or network's administration or maintenance.
- ◆ Perform certification a minimum of once every three years due to the changing nature of computer systems and accelerating rate of change of IT-related security risks.

AMC/HIPAA Workgroup

- ◆ Prepare a formal “Certification and Accreditation Report” upon the completion of certification and forward it, along with any recommendations on accreditation, to the accrediting official.
- ◆ Maintain records and reports of certification and accreditation activities for the last two certification efforts to provide for an adequate history of certification information and an audit trail of certification.
- ◆ Establish routine testing, auditing, and change management procedures to support the certification process.
- ◆ Consider certification for system changes prior to placing such systems into production.
- ◆ Consider a phased approach to certification in order to encourage continuity of the process.
- ◆ Consider linking the certification process to JCAHO Information Management requirements.
- ◆ Consider requiring formal security credentials for those conducting the certification process.

Roadblocks

In complex institutions, it may be difficult to establish the necessary credibility and authority for the certifier.

Comments

Although the evaluation of the program or one of its parts may be done by outside entities, the certification is a statement by senior management of the institution. State law on record-keeping may mandate additional retention requirements. Covered entities should be prepared to budget for remedial action as necessary if deficiencies are discovered during the certification process.

AMC/HIPAA Workgroup

SEC.02 Chain of Trust Partner Agreement § .308(a)(2)

HIPAA Requirement

A chain of trust partner agreement (a contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged).

AMC Explanation of HIPAA Regulation

A Chain of Trust Agreement is required between two business partners whenever data is electronically exchanged. The Agreement requires that the sender and the receiver of the protected health information work with each other to maintain the information's integrity and confidentiality. Such contracts provide a legal basis for maintaining consistent levels of data integrity and confidentiality.

Key Issues

- ◆ With which persons or organizations is the health care provider, health plan, or health care clearinghouse required to execute a Chain of Trust Agreement (COT)?
- ◆ Is there a documented process for identifying all partners with which a COT is required?
- ◆ Does the COT identify a process or processes to ensure the integrity and confidentiality of the data transmitted?
- ◆ How will security responsibilities and accountabilities be determined, drafted, and monitored?
- ◆ Does more than one unit have the authority to contract with a business partner?
- ◆ Is there a process in place to assure that all AMC contracts have the required and appropriate language?
- ◆ Is there a process that will identify the data rights of the trading partners and incorporate such rights in the COT language?
- ◆ Does the agreement identify appropriate sanctions for failure to abide by its terms?
- ◆ Is the duration of the agreement appropriate?
- ◆ Is there a process in place to assure that all AMC contracting officers are aware of the need for, and know the requisites of, an effective COT?
- ◆ What organizational unit will be responsible for managing the COT policy implementation?
- ◆ Does the COT propagate with any further transfers of information between partners and their other partners?
- ◆ Does the COT survive other agreements with the partner?
- ◆ How do COTs relate to the business associate contractual terms in the Privacy rule?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop a Chain of Trust Agreement with each party with which protected health information is shared, including language that states that:
 - ▶ The parties agree to electronically exchange data and protect the transmitted data; and
 - ▶ Each party will maintain the integrity and confidentiality of the transmitted information.

AMC/HIPAA Workgroup

- ◆ Develop a plan to update all current agreements to ensure that the terms and conditions do not contain any provisions, including data content and format definitions, that conflict with the standards outlined in the security regulations
- ◆ Develop a plan to ensure that all future agreements have appropriate provisions.

Category II Guidelines-Actions should be taken to address these

- ◆ Engage legal counsel to develop and review contract language for the COT.
- ◆ Establish monitors to ensure compliance by all parties subject to the agreement.
- ◆ Train all contracting officials about the nature and intent of the COT.
- ◆ Devise and promulgate a COT template for all Contracting Officers to use.
- ◆ Establish a process to determine when/how to activate the sanctions for nonperformance with regard to COT.
- ◆ Periodically review all current partnerships for COT need.
- ◆ Develop process to review partners' COTs for adequacy and fairness.

Roadblocks

It will likely be difficult to get approval for COTs which are inconsistent between partners, or which are perceived as unbalanced in responsibility. Contracts are frequently negotiated and approved by various departments within the University or AMC. Each area within the University and AMC must be trained as to when and with whom this required language should be used.

Comments

Since the originator of information bears the responsibility for improper disclosure or other security failures regarding that information, a COT is the only protection most providers will have once information is turned over to their partners in healthcare provision.

As part of a compliance program, business associates should warrant, and the AMC department responsible for negotiating and signing the Agreement should verify, that the trading partner is not excluded from participation in any government program. Contracts should also include a statement that the trading partner warrants that any subcontractors or agents are not excluded from participation in any government program.

The Chain of Trust Agreement in the Supplement contains language that can be used to satisfy both the proposed security regulation (discussed in this point) and the final privacy regulation (discussed in PRIV.03).

SEC.03 Contingency Planning § .380 (a)(3)

HIPAA Requirement

...a routinely updated plan for responding to a system emergency, that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. The plan must include all of the following implementation features:

(i) An applications and data criticality analysis [an entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits].

(ii) Data backup plan (a documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information).

(iii) A disaster recovery plan (the part of an overall contingency plan that contains a process enabling an enterprise to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure).

(iv) Emergency mode operation plan (the part of an overall contingency plan that contains a process enabling an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure).

(v) Testing and revision procedures (the documented process of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary).

AMC Explanation of HIPAA Regulation

Each covered entity is required to maintain a contingency plan for responding to system emergencies involving systems that contain protected health information. The covered entity is required to perform periodic backups of data, have critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place for such systems. Systems that do not involve protected health information are not required to have contingency plans.

Key Issues

- ◆ What will be needed to recreate each data element in the event of an emergency? Has an assessment been performed?
- ◆ What is the appropriate frequency and depth of backups?
- ◆ Where should backup data be located?
- ◆ How easy is restoration of backup data?
- ◆ How timely would such a restoration be?
- ◆ How is security of data assured at the backup location?
- ◆ What is the mechanism for testing the plans and procedures?
- ◆ How long will backups be retained?
- ◆ How is overall integrity of data assured?
- ◆ How often will various levels or types of tests be performed?

AMC/HIPAA Workgroup

Category I Guidelines-Actions must be taken to address these

- ◆ Assess all systems with protected health information for reasonably anticipated risks, focusing on the potential impact of the lack of availability of specific applications and data on the secure operation of the covered entity.
- ◆ Prepare a data backup plan that details how data will be maintained and duplicated in order to prevent its loss during a natural or man-made disaster.
- ◆ Prepare a disaster recovery plan that details how data and operations would be restored in a timely fashion following a catastrophic event or unanticipated interruption of operations.
- ◆ Prepare a plan to use for emergency operations following a catastrophic event until normal operations can be restored.
- ◆ Test these procedures periodically and revise them accordingly to address any weaknesses discovered during testing.

Category II Guidelines-Actions should be considered to address these

- ◆ Develop a data storage plan that ensures that the medium and location of backup storage are secure from physical damage and that backup storage is separated in some way from the main site.
- ◆ Dispose of information in a manner that maintains its security. Shred paper and wipe magnetic or optical media.
- ◆ Make backups at regular intervals.
- ◆ Develop a procedure covering the scope (full, incremental, and differential) of backups.
- ◆ Provide adequate facilities to support recovery operations.
- ◆ Test contingency and disaster recovery plans regularly, specifically including restoration of data.
- ◆ Protect backup information at the same level as the original data.

Roadblocks

Identifying and testing critical components may be more realistic and cost effective than testing plans sufficiently often to ensure that they are viable.

Formal disaster recovery/contingency plans usually occur at the level of central IT within an AMC. The distributed nature of support and systems within an AMC may serve as a roadblock to ensuring consistent planning.

Comments

The security regulations (unlike the privacy regulations) supersede conflicting state laws. Non-conflicting state laws, however, still apply and may affect various aspects of this plan.

Also see: AMC.09 Stricter State Law, SEC.14 Media Controls

AMC/HIPAA Workgroup

SEC.04 Formal Mechanism for Processing Records § .308(a)(4)

HIPAA Requirement

Formal mechanism for processing record (documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information).

AMC Explanation of HIPAA Regulation

Covered entities are required to maintain documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of protected health information.

Key Issues

- ◆ Do clear lines of authority and responsibilities exist that fit the structure and function of entities (Hospital, Departments, Sections)?
- ◆ Are there provisions for evaluating and improving policies and procedures at all levels?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop and document processes to govern the creation of protected health information.
- ◆ Establish policies and procedures on storage of data, including administrative policies governing the length of time to various types of data are to be stored and policies for the archiving and destruction of data.
- ◆ Establish policies for data dissemination within and external to the covered entity. (See Comments.)
- ◆ Develop policies for secure disposal of protected health information, including information contained on media and systems that are replaced.

Category II Guidelines-Actions should be taken to address these

- ◆ Protect records to a degree commensurate with the risk associated with them.
- ◆ Consider standardizing record management policies across the enterprise.

Roadblocks

The presence of already existing unofficial systems may act as a barrier to change, as these will need to be brought under the umbrella of protection. If staff do not accept needed changes, then implementation may be delayed.

Redundancy of records in multiple systems presents a challenge, with updates in one system not always filing or updating correctly in other systems downstream.

Comments

Policies external to the covered entity may be problematic in terms of generality or specificity. Standards, such as message types (HL7, XML, etc.) may help in this regard.

SEC.05 Information Access and Control § .308(a)(5)

HIPAA Requirement

...(formal, documented policies and procedures for granting different levels of access to health care information) that includes all of the following implementation features:

(i) Access authorization (information-use policies and procedures that establish the rules for granting access, for example, to a terminal, transaction, program, process, or some other user.)

(ii) Access establishment (security policies and rules that determine an entity's initial right of access to a terminal, transaction, program, process or some other user).

(iii) Access modification (security policies and rules that determine the types of, and reasons for, modification to an entity's established right of access, to a terminal, transaction, program, process, or some other user.)

AMC Explanation of HIPAA Regulation

Each covered entity is required to establish and maintain formal, documented policies and procedures for granting different levels of access to protected health information. These policies and procedures must, at a minimum, include:

- ◆ Access authorization policies and procedures;
- ◆ Access establishment policies and procedures; and
- ◆ Access modification policies and procedures.

Key Issues

- ◆ Does the covered entity currently have a documented access control policy?
- ◆ Is there a process to establish an individual right-to-know and/or need-to-know?
- ◆ Does the access control policy consider all means of access?
- ◆ Do procedures define the authorization requirements for various forms of protected health information, and is special authorization required for more sensitive information (e.g., psychiatry, infectious diseases, genetic disorders)?
- ◆ Is access authorization documented and maintained?
- ◆ Is there a documented process for revoking access?
- ◆ How does the covered entity authorize, implement, and revoke emergency access?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish documented policies and procedures to assign, implement, revoke, and modify access to protected health information.

Category II Guidelines-Actions should be taken to address these

- ◆ Create a process for determining access needs for individuals and other entities such as law enforcement and public health.
- ◆ Grant access on the basis of need-to-know and/or right-to-know.

AMC/HIPAA Workgroup

- ◆ Provide a means to review the effectiveness of access management and control.
- ◆ Assign responsibility for implementing the policy to specific individuals or organizations within the covered entity.
- ◆ Enact a process to modify access, taking into account the types of, and reasons for, previously established access.
- ◆ Require implementation of technical means to control information access.
- ◆ Require execution of a grantor-grantee agreement to honor information security requirements before access is granted.
- ◆ Establish a process to ensure that system access is available at appropriate times for repair and other maintenance purposes.
- ◆ Establish a documented plan to ensure that all workforce members can demonstrate knowledge of access control responsibilities and how to obtain access authorization.
- ◆ Establish a process whereby termination of a workforce member or other entity's need for data access will trigger timely revocation of access.
- ◆ Require data owners or stewards to list functions that will require access to data for which they are responsible.

Roadblocks

Any part of the access control process can be rendered ineffective if those with access do not respect the process — if the users do not understand their responsibilities and buy in to the program, it will not work.

Comments

Also see: SEC.19 Access Control

Access control requirements appear throughout the security regulations in a number of different contexts relating to personnel security requirements, physical safeguards, technical security services, and technical security mechanisms. Access control is an integral part of almost every element of information security. Vulnerabilities in this area include *ad hoc* practices and/or incomplete policies and procedures for authorizing and establishing access to organizational systems, failure to include smaller departmental systems in access control policies and practices, and broken processes to address the modification and revocation of user access following job changes or termination.

SEC.06 Internal Audit § .308(a)(6)

HIPAA Requirement

...in-house review of the records of system activity (such as logins, file accesses, and security incidents) maintained by an organization.

AMC Explanation of HIPAA Regulation

This requirement calls for periodic reviews of a covered entity's internal security controls, including records of logins, file accesses, and security incidents.

Key Issues

- ◆ At what level in data structures should audits be maintained? Table? Record? Field?
- ◆ How will this degrade system performance?
- ◆ For what data will logs be maintained, and for how long?
- ◆ Who will review the records? (The log itself may have protected health information in it.)
- ◆ How much of the review can be done by software?
- ◆ How often will audits occur?
- ◆ What logged activity will be considered suspicious?
- ◆ What actions will be taken in response to suspicious audit information?

Category I Guidelines-Actions must be taken to address these

- ◆ Maintain, and periodically review, audit trails or activity logs for critical application systems, including user-written applications.

Category II Guidelines-Actions should be taken to address these

- ◆ Follow up on suspicious entries such as unauthorized accesses and access attempts.
- ◆ Identify and resolve inappropriate activity.
- ◆ Ensure that audit procedures validate the necessity for data input, processing, and output.
- ◆ Ensure that audit requirements and activities do not disrupt important business processes.
- ◆ Agree to and control the scope of the checks.
- ◆ Explicitly identify resources for performing the checks and ensure that they are available.
- ◆ Identify and agree to requirements for special or additional processing, such as prospective audits of user activity.
- ◆ Document all procedures, requirements, and responsibilities.
- ◆ Consider making logs of access to individuals' health information available to the subjects of the records via a "patient portal."
- ◆ Develop an audit process to ensure that users comply with access control procedures.

Roadblocks

Users, in carrying out their respective duties, should never feel threatened by an audit. In most cases, information systems personnel are checking a system for problem-solving purposes and it remains transparent to the user. If the user is made aware, it is usually for the purpose of problem solving or procedure correction.

AMC/HIPAA Workgroup

Comments

The logs themselves may contain protected health information and should be appropriately secure. Additional controls may be required for systems that process or have an impact on sensitive, valuable, or critical organizational assets. Such controls should be determined on the basis of security requirements and a formal risk assessment. Audit trails may become evidence in legal proceedings, so care should be taken to protect their integrity in order to preserve their usefulness for such purposes. Take the possibility of using audit trails as evidence into account when deciding how long they should be retained. Prospective audits are onerous and usually require clinician input to resolve need-to-know issues; they should be performed sparingly and only with good cause as determined through the risk analysis process.

Audits can be a significant cost consideration and logging records could have an unreasonable cost impact. A cost/benefit and risk analysis would be in order to determine what systems should employ logging and how long the records should be stored.

Formal audit log retention standards are prudent. Destruction of log data should not appear to be an attempt to destroy evidence in the case of legal action.

Also see: SEC.20 Audit Controls.

SEC.07 Personnel Security § .308(a)(7)

HIPAA Requirement

...(all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances) that includes all of the following implementation features:

Assuring supervision of maintenance personnel by an authorized, knowledgeable person. These procedures are documented formal procedures and instructions for the oversight of maintenance personnel when the personnel are near health information pertaining to an individual.

Maintaining a record of access authorizations (ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information).

Assuring that operating and maintenance personnel have proper access authorization (formal documented policies and procedures for determining the access level to be granted to individuals working on, or near, health information).

Establishing personnel clearance procedures (a protective measure applied to determine that an unclassified automated information is admissible).

Establishing and maintaining personnel security policies and procedures (formal, documentation of procedures to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances).

Assuring that system users, including maintenance personnel, receive security awareness training.

AMC Explanation of HIPAA Regulation

Each covered entity must establish a personnel security clearance process to administratively determine that persons and computers are trustworthy before giving them access to protected health information. This process must account for, and document, levels of access granted to individuals, programs, and procedures. The process must also address persons who fill roles where incidental access to protected health information may occur, such as system and network support and maintenance personnel. Supervision of uncleared or unauthorized personnel, such as support and maintenance personnel, is necessary unless their access to protected health information can be precluded. Awareness training on these policies and procedures is required both for those who are cleared for and given access and those who have incidental access.

Key Issues

- ◆ How closely must maintenance personnel be supervised?
- ◆ How often should procedures, instructions, and levels of access be reviewed?
- ◆ How broad, or how specific, should security training be? What should it cover?
- ◆ How often should security training be repeated for employees? For vendors and other contracting personnel?

AMC/HIPAA Workgroup

Category I Guidelines-Actions must be taken to address these

- ◆ Establish written personnel clearance procedures for determining the appropriateness of access to protected health information or systems.
- ◆ Maintain documentation regarding the levels of access granted to each individual, program, and procedure.
- ◆ Review access levels periodically.
- ◆ Review access levels when the status of the workforce member changes.
- ◆ Ensure that system users and technical maintenance staff receive security awareness training.
- ◆ Ensure that maintenance and vendor personnel are supervised when working on or near protected health information.

Category II Guidelines-Actions should be taken to address these

- ◆ Conduct records checks on applicants for employment, including residence, employment, criminal history, and education, when job requires access to protected health information. (See Comments.)
- ◆ Require staff and maintenance/vendor employees to sign non-disclosure statements before being given access to protected health information.

Roadblocks

Workforce member status changes can be difficult to track in a large covered entity. Consistent application of personnel access policies may be problematic when protected health information is shared between institutions.

Comments

The personnel clearance process is an administrative determination of trustworthiness. Human Resources normally performs this function in AMCs. A nominal records check should ascertain that an individual is not falsifying identity, previous employment or education, or any professional certifications. Additionally, any potentially disqualifying criminal activity should be discovered. Federal criminal records are centralized in the FBI database, but state and local records are largely unlinked. It is therefore necessary to determine where individuals have resided in order to check state and local criminal records in disparate jurisdictions. Arrest and conviction data is public information and available on request.

SEC.08 Security Configuration Management § .308(a)(8)

HIPAA Requirement

...(measures, practices, and procedures for the security of information systems that must be coordinated and integrated with each other and other measures, practices, and procedures of the organization established in order to create a coherent system of security) that includes all of the following implementation features:

- (i) Documentation (written security plans, rules, procedures, and instructions concerning all components of an entity's security).*
- (ii) Hardware and software installation and maintenance review and testing for security features (formal, documented procedures for connecting and loading new equipment and programs, periodic review of the maintenance occurring on that equipment and programs, and periodic security testing of the security attributes of that hardware/software).*
- (iii) Inventory (the formal, documented identification of hardware and software assets).*
- (iv) Security testing (process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment; this process includes hands-on functional testing, penetration testing, and verification).*
- (v) Virus checking. (The act of running a computer program that identifies and disables:
 - (A) Another "virus" computer program, typically hidden, that attaches itself to other programs and has the ability to replicate.*
 - (B) A code fragment (not an independent program) that reproduces by attaching to another program.*
 - (C) A code embedded within a program that causes a copy of itself to be inserted in one or more other programs.)**

AMC Explanation of HIPAA Requirement

A covered entity is required to have written security plans and procedures guiding its security efforts so as to create a comprehensive security program. The security program must include an inventory of system assets, formal procedures for installing and testing new systems, a regular security testing schedule, and virus checking.

Key Issues

- ◆ How can a covered entity identify all components of its security features?
- ◆ How should inventory be reviewed and updated—when assets are added and removed or on a routine schedule?
- ◆ At what levels should virus scans be run? Servers? Mail hubs?
- ◆ How often should virus scans be run?
- ◆ How often should virus detection programs be updated?
- ◆ How frequently should security testing, such as penetration testing, occur?

AMC/HIPAA Workgroup

Category I Guidelines-Actions must be taken to address these

- ◆ Develop written security plans, procedures, and instructions to cover all areas of the covered entity's information security needs.
- ◆ Create and document procedures for installing and maintaining software and hardware and periodic testing of that software and/or hardware's security attributes.
- ◆ Develop a written inventory of hardware and software assets and keep the inventory current.
- ◆ Conduct security testing to ensure that the covered entity's security features are adequate; security testing must include a manual or automated process of identifying vulnerabilities, functional and penetration testing, and verification.
- ◆ Ensure that virus scans are run on a regular schedule.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish a team representing diverse perspectives to plan security controls.
- ◆ Have written procedures to report equipment malfunctions and any remedial actions taken.
- ◆ Require departmental systems not managed centrally to comply with the same security configuration requirements as centrally managed systems.
- ◆ Employ anti-virus countermeasures at multiple levels, for example on servers, e-mail hosts, and desktops.
- ◆ Maintain a separate test environment and test system changes for security integrity there before moving them to the production systems.

Roadblocks

A single, well-integrated security plan is difficult to establish in an institution with hundreds of distributed, heterogeneous systems using a wide range of technologies. The plan should be multi-tiered and well coordinated. Even identifying all departmental systems with patient information may be difficult in a decentralized AMC.

Comments

AMCs may want to consider coordinating their inventory reviews with accreditation agency standards and reviews.

SEC.09 Security Incident Procedures § .308(a)(9)

HIPAA Requirement

...(formal documented instructions for reporting security breaches) that include all of the following implementation features:

- (i) Report procedures (documented formal mechanism employed to document security incidents).*
- (ii) Response procedures (documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report).*

AMC Explanation of HIPAA Regulation

The covered entity must have written procedures for reporting security breaches to ensure that security violations are handled promptly and appropriately. These must include:

- ◆ Procedures for reporting security incidents.
- ◆ Procedures describing response, i.e. actions to take when a security incident is reported.

Key Issues

- ◆ What constitutes a security incident?
- ◆ How should the covered entity define levels of incidents and sanctions for each (e.g., accessing protected health information as opposed to sharing protected health information)?
- ◆ How can security awareness be kept “hot?”
- ◆ How can a covered entity determine when access to protected health information is inappropriate?

Category I Guidelines-Actions must be taken to address these

- ◆ Implement an incident reporting and response procedure and document it.

Category II Guidelines-Actions should be taken to address these

- ◆ Tell workforce members when, how, and to whom to report a security incident.
- ◆ Require workforce members to acknowledge that they have received security incident training.
- ◆ Require workforce members to report the incident if they inadvertently access protected health information they should not have accessed.
- ◆ Ensure that workforce members know that they should report security violations to a supervisor, system administrator, security, internal audit, or others as appropriate.
- ◆ Require workforce members to report instances of noncompliance.
- ◆ Ensure that the teams of people who are typically involved in responding to a security incident have a well-understood working arrangement that ensures that the incident is handled efficiently, expeditiously, and with respect for law and individual rights.

Roadblocks

Communications between different organizational units within an AMC can be poor. Covered entities should make sure that their IT organizations share information about security incidents

AMC/HIPAA Workgroup

with each other in a timely manner, and may need to set up mechanisms to ensure that this happens.

Determining where potential security breaches may occur is challenging. For instance, physicians may download medical data onto personal digital assistants. They often purchase such devices themselves, and Security Management has no way of knowing about the purchase or whether the physicians are adhering to security standards.

Comments

Also see: PRIV.53 Sanctions.

SEC.10 Security Management Process § .308(a)(10)

HIPAA Requirement

...(creation, administration, and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches involving risk analysis and risk management). It includes the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets (both physical and electronic) that includes all of the following implementation features:

(i) Risk analysis, a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.

(ii) Risk management (process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk).

(iii) Sanction policies and procedures (statements regarding disciplinary actions that are communicated to all employees, agents, and contractors; for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment, and contract penalties). They must include employee, agent, and contractor notice of civil or criminal penalties for misuse or misappropriation of health information and must make employees, agents, and contractors aware that violations may result in notification to law enforcement officials and regulatory, accreditation, and licensure organizations.

(iv) Security policy (statement(s) of information values, protection responsibilities, and organization commitment for a system). This is the framework within which an entity establishes needed levels of information security to achieve the desired confidentiality goals.

AMC Explanation of HIPAA Regulation Key Issues

An overall information security management process is necessary to establish policy, provide oversight, and administer operational aspects of the program. The process must function in a proactive, risk-appropriate manner and establish the framework for safeguarding protected health information within the AMC. An over-arching information security policy that commits the AMC to safeguard protected health information, to establish goals, and to assign responsibility is necessary. Supporting policy statements and procedures are required to facilitate the prevention, detection, containment, and correction of security breaches. Specific areas that the security management process must cover are: risk analysis process, risk management process, sanction process, and security policy.

Key Issues

- ◆ What are the covered entity's values with regard to protecting information?
- ◆ What are the covered entity's security goals?
- ◆ How does the covered entity's security policy demonstrate commitment to these goals?
- ◆ How will values, policy, and process be effectively communicated to those covered by them?

AMC/HIPAA Workgroup

- ◆ What activities can not be managed in a secure way?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish a management structure that identifies roles and responsibilities for security oversight and operational aspects.
- ◆ Establish an overall information security policy that articulates the organization's priorities and expectations with respect to safeguarding protected health information.
- ◆ Identify and communicate security responsibilities of workforce member who access or manage access to protected health information.
- ◆ Employ risk analysis to identify information assets, threats, and the likelihood and costs of adverse occurrences.
- ◆ Manage risk by applying cost-effective security solutions to reduce likelihood and extent of losses due to adverse occurrences.
- ◆ Develop a sanctioning process for violators and communicate it to all workforce members. In addition to institutional corrective action, the policy must include notices of civil or criminal penalties and notices that violations may result in notification of law enforcement, and/or regulatory, accreditation, and licensure organizations.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop and apply a data criticality/sensitivity classification scheme.
- ◆ Make risk analysis and risk management ongoing.
- ◆ Consider establishing progressive sanctions, such as verbal warning, written warning, suspension, and employment termination.
- ◆ Ensure that the sanction policy provides for swift and strong action when appropriate.
- ◆ Establish a process to document and evaluate trends in breaches and sanctions in order to identify potential improvements in security, e.g. changes to policy, procedures, training, or technical measures.
- ◆ Require all who have, or may have, access to protected health information to sign security, confidentiality, and computer usage agreements.

Roadblocks

Developing and implementing consistent policies and procedures for sanctions and security policy may be hindered by the typical AMC's decentralized structure and culture of autonomy (academic freedom). At some AMCs, these policies may also have to be coordinated with the associated university's central administration, especially its legal counsel's office and human resources department.

Comments

The reader is referred to the following additional references:

Carnegie Mellon University
Software Engineering Institute
Computer Emergency Response Team Coordination Center (Cert/CC)
<http://www.cert.org/octave/>

AMC/HIPAA Workgroup

Information Security Risk Evaluation

CPRI-Toolkit for Managing Information Security in Healthcare

<http://www.3com.com/healthcare/securitynet/hipaa/toc.html>

Health Information Risk Assessment and Management

SEC.11 Termination Procedures § .308(a)(11)

HIPAA Requirement

...(formal documented instructions, which include appropriate security measures, for the ending of an employee's employment or an internal/external user's access) that include procedures for all of the following implementation features:

- (i) Changing locks (a documented procedure for changing combinations of locking mechanisms, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or require access to the protected facility or system).*
- (ii) Removal from access lists (physical eradication of an entity's access privileges).*
- (iii) Removal of user account(s) (termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists).*
- (iv) Turning in of keys, tokens, or cards that allow access (formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably before termination).*

AMC Explanation of HIPAA Regulation

Entities must revoke physical access to controlled areas and remove user accounts when employees terminate employment or when others, such as contractors and vendors, no longer require access. Academic medical centers can reduce risk by implementing procedures to ensure prompt collection of the items that enable access: e.g., identification cards, keys, and physical tokens, and by changing locks or lock combinations, and by revoking computer accounts. Although this point is entitled "termination," the text includes provisions for other occasions in which removal of access rights is called for.

Key Issues

- ◆ Is access disabled in a timely and consistent manner for terminated users?
- ◆ Is there timely notification to: human resources, central security administration, decentralized security administrators, when an employee is terminated?
- ◆ Is there a way to deal with terminations of individuals who are not employees, e.g. physicians, contractors, vendors, volunteers? Are there provisions to modify/remove access when workforce members change roles in ways that imply change in access privileges?

Category I Guidelines-Actions must be taken to address these

- ◆ When workforce members either terminate employment or lose clearance, or their authorization or need-to-know no longer exists, take the following actions:
 - ▶ Recover keys, identification cards, physical tokens, and any other objects that facilitate physical access to property, buildings, and equipment;

AMC/HIPAA Workgroup

- ▶ Change locks and/or combinations that control physical access to areas and equipment (this must also be done on a recurring basis);
- ▶ Revoke user accounts that provide access to information, services, and resources;
- ▶ Remove them from lists that document authorized access to controlled areas and information, services, and resources;
- ▶ Document these processes as formal instructions.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish a policy and process to promptly report all terminations and ensure that the revocation process works promptly.
- ◆ Document explicit maximum time intervals that are permissible for:
 - ▶ Reporting terminations;
 - ▶ Communicating terminations to security administrators;
 - ▶ Disabling access.
- ◆ Develop and document a process to ensure that, in instances of involuntary termination, the action is immediately reported to security administrators and that items that enable access are collected or inactivated immediately.
- ◆ Consider revoking access prior to employment termination, particularly in instances of involuntary termination.
- ◆ Consider conditions in which people put on administrative leave (e.g. pending an investigation of misuse of access) should have their access privileges altered.
- ◆ Revise access when roles change.
- ◆ Disable access privileges for any user account that shows no activity for a pre-determined period of time (e.g. three months).
- ◆ Review all suspended accounts for activity or attempted activity and report any such activity for investigation as a potential breach.
- ◆ Periodically audit the effectiveness of the process for disabling access in the event of a termination to ensure that procedures and guidelines are being followed.
- ◆ Record the completion of inactivation activities.
- ◆ Perform exit interviews for any termination in which a potential security concern has been identified.
- ◆ Maintain a record of any changes made to an individual's access privileges, and retain it long enough so it is possible to determine the extent of an individual's historic access in case it is relevant to an investigation.

Roadblocks

AMCs often have a decentralized structure and culture, and thus have many computer systems with decentralized management. Take into consideration that AMCs often have many sites with controlled physical access.

Comments

Linkage of HR, Payroll, and IT systems is a major step in resolving this difficult issue. Education, procedures, and checklists for managers on terminating staff are essential for a successful termination process.

SEC.12 Security Training § .308(a)(12)

HIPAA Requirement

...(education concerning the vulnerabilities of the health information in an entity's possession and ways to ensure the protection of that information) that includes all of the following implementation features:

- (i) Awareness training for all personnel, including management personnel (in security awareness, including, but not limited to, password maintenance, incident reporting, and viruses and other forms of malicious software).*
- (ii) Periodic security reminders (employees, agents, and contractors are made aware of security concerns on an ongoing basis).*
- (iii) User education concerning virus protection (training relative to user awareness of the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected).*
- (iv) User education in importance of monitoring log-in success or failure and how to report discrepancies (training in the user's responsibility to ensure the security of health care information).*
- (v) User education in password management (type of user training in the rules to be followed in creating and changing passwords and the need to keep them confidential).*

AMC Explanation of HIPAA Regulation

Security training is necessary for all workforce members who access protected health information. This training must include overall security awareness, periodic reminders, virus awareness, password management, and user-specific topics necessary for individual workstation security.

Key Issues

- ◆ How will the security training program be updated to reflect changes in the security environment and security responsibilities of workforce members?
- ◆ How is the training program tailored to support the various classes of system users and the level of information sensitivity to which each class of user has access?
- ◆ Are all system users included in the training program, including those accessing organizational systems from remote sites?
- ◆ How is training documented?
- ◆ How is training effectiveness evaluated?
- ◆ Does the training content meet all of the HIPAA training requirements?
- ◆ How often should reminders or refresher courses be provided?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish a formal, documented security awareness training program for all workforce members that addresses, at a minimum, the following topics:
 - ▶ Protection against, and reporting of, viruses;

AMC/HIPAA Workgroup

- ▶ Reporting security incidents;
- ▶ Managing individual passwords.
- ◆ Establish a formal, documented security awareness program tailored to system users that addresses, at a minimum:
 - ▶ Virus protection;
 - ▶ Potential harm viruses can cause;
 - ▶ How to prevent the introduction of viruses into a computer system;
 - ▶ What to do if a virus is detected;
 - ▶ The importance of monitoring log-in success or failure;
 - ▶ How to report discrepancies in the log-in process;
 - ▶ Rules for creating and changing passwords;
 - ▶ Safeguarding passwords.
- ◆ Provide periodic security awareness reminders to all workforce members.

Category II Guidelines-Actions should be taken to address these

- ◆ Make training role and/or job-specific.
- ◆ Assign responsibility for security training.
- ◆ Document the training that has been provided to each individual.
- ◆ Develop a training program that demonstrates mastery of the material presented.
- ◆ Evaluate the effectiveness of training.

Roadblocks

Security training is generally not given a high priority in orientation and training for new hires, so the time available may be inadequate. It is also often difficult to arrange security training for third-party agents and sub-contractors with access to health information. Without centralized responsibility for the development of content for the security program, it will be difficult to ensure consistent training across the AMC.

Comments

Using experts in this field will enhance the content of security training programs. Some AMCs reduce the costs of security training by weaving training into ongoing training activities. Consider including a security training curriculum for residents, as well as for medical and nursing students.

Also see: SEC.18 Security Awareness Training.

The reader is referred to the following additional references:

American Health Information Management Society

<https://secure.ahima.org/commerce/>

- Faxing Safeguards: Guidelines For Transmitting Patient Health Information
- Security And Access: Guidelines For Managing Electronic Patient Information
- Information Security: HIPAA Sets The Standard Program In A Box

Carnegie Mellon University

AMC/HIPAA Workgroup

Software Engineering Institute

Computer Emergency Response Team Coordination Center (Cert/CC)

<http://www.cert.org/nav/training.html>

Computer Security Institute, Manager's Guide to Computer Security Awareness

<http://www.gocsi.com/>

CPRI-Toolkit for Managing Information Security in Healthcare

<http://www.3com.com/healthcare/securitynet/hipaa/toc.html>

- CPRI Guide - Information Security Education
- Instructor Guide
- Slides for Training Program

MIS Training Institute

<http://www.misti.com/>

National Institutes of Health Web Security Links

<http://www.alw.nih.gov/Security/security.html>

National Institute of Standards and Technology (NIST)

Computer Security Resource Center

<http://csrc.ncsl.nist.gov/>

AMC/HIPAA Workgroup

Section Two: Requirements for Physical Safeguards

SEC.13 Assigned Security Responsibility § .308(b)(1)

HIPAA Requirement

...(practices established by management to manage and supervise the execution and use of security measures to protect data and to manage and supervise the conduct of personnel in relation to the protection of data).

AMC Explanation of HIPAA Regulation

The governing body of each covered entity must designate a security officer or group to oversee the safeguarding of protected health information and assign the necessary responsibility and accountability to that role. This person or group will manage the execution and use of security measures and supervise the conduct of personnel in relation to data protection.

Key Issues

- ◆ Will the covered entity instill this responsibility in an individual role or charge a committee?
- ◆ How will the covered entity empower the security officer or group to effectively accomplish security goals?
- ◆ How will multiple facility entities assign oversight?
- ◆ How will multiple entity systems assign oversight?

Category I Guidelines-Actions must be taken to address these

- ◆ Assign overall responsibility for securing protected health information to an individual security officer or a group specifically charged to do so.
- ◆ Make this person or group accountable for the information security program to include:
 - ▶ Processes employed to safeguard protected health information;
 - ▶ Technologies and architectures employed to safeguard protected health information;
 - ▶ Conduct of personnel in relation to the safeguarding of protected health information.

Category II Guidelines-Actions should be taken to address these

- ◆ Have the organization's governing body assign this responsibility and instill the authority to effectively accomplish the task.
- ◆ Ensure that the security officer possesses the necessary body of knowledge, skill set, and experience to effectively oversee the security program.
- ◆ Extend the security officer's responsibility to the entire entity.
- ◆ If the organization has multiple security officers, coordinate their efforts.
- ◆ Avoid combining the responsibilities of the security officer and the privacy official, as the knowledge bases and skill sets required for each differ.

Roadblocks

Security officers with the knowledge, skills, and experience necessary to effectively manage an information security program in an AMC are few and difficult to recruit. On the other hand, training a person with a general or non-healthcare information security background on the job takes a good deal of time.

AMC/HIPAA Workgroup

Comments

None.

SEC.14 Media Controls § .308(b)(2)

HIPAA Requirement

...(formal, documented policies and procedures that govern the receipt and removal of hardware/software (such as diskettes and tapes) into and out of a facility) that include all of the following implementation features:

Access control.

Accountability (the property that ensures that the actions of an entity can be traced uniquely to that entity).

Data backup (a retrievable, exact copy of information).

Data storage (the retention of health care information pertaining to an individual in an electronic format).

Disposal (final disposition of electronic data, and/or the hardware on which electronic data is stored).

AMC Explanation of HIPAA Regulation

While this item states that it is focused upon the transfer of hardware and software media into and out of a facility, it also requires consideration of the larger issue of how to handle record copies of protected media from creation to destruction. Each entity will need to decide how to categorize, annotate, account for, store, and dispose of protected health information in record form.

Key Issues

- ◆ How and by whom is new media introduced into the record environment?
- ◆ How are working materials created, marked, controlled, and destroyed?
- ◆ How are media and computer equipment controlled when entering and leaving the facility?
- ◆ Is equipment properly inventoried?
- ◆ Is media disposed of properly?
- ◆ Do the use of unofficial and “shadow” record systems undermine accountability and controls and, if so, how can they be brought into line with media controls?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish accountability and access controls for media containing protected health information, including equipment with media installed and hardcopies containing protected health information, from creation to disposition.
- ◆ Ensure that policies and procedures address access control, accountability, data backup, data storage, and data disposal.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish uniform terminology and guidelines for classifying and marking materials as “confidential,” “proprietary,” “patient-confidential,” etc.

AMC/HIPAA Workgroup

- ◆ Establish procedures for assigning accountability for newly created media, including hardcopy when created and recording/removing the media from accountability when properly destroyed.
- ◆ Establish guidelines to restrict the use of “unofficial” or “shadow” records to ensure the integrity and protection of protected health information.
- ◆ Mark temporary working materials, whether on computer media or hard copy, that contain protected health information appropriately when created and establish a date for either destroying the working materials or bringing them under control as record documents.
- ◆ Ensure that appropriate secure storage and destruction facilities, such as shredders, are readily available, clearly marked, and used.
- ◆ Ensure that protected health information in hardcopy format is disposed of properly.
- ◆ Responsible personnel should authorize the shipping and receiving of protected media and maintain appropriate records. Establish a formal system for shipping and transporting materials containing protected health information with receipts to ensure that shipped materials have been properly received and accountability has been transferred to the receiving office. Establish standards for wrapping and marking shipped media that both minimize the likelihood of its being identified as containing protected health information and prevent tampering.
- ◆ Set a standard for purging protected health information from magnetic media, and adhere to it. Degaussing and overwriting are acceptable methods. (See Comments.)
- ◆ Before releasing any magnetic media that may contain protected health information outside the entity, process it to purge any information residing on it.
- ◆ If media is left unattended, secure it and use reasonable care.
- ◆ Do not leave printed versions (hardcopy) of protected health information unattended and open to compromise, and do not copy it indiscriminately.
- ◆ Establish and maintain accountability for all equipment used to process protected health information, including requirements for regular inventory and resolving any loss of accountability.
- ◆ Ensure that essential patient care information is properly backed up in a secure location. Periodically check to ensure that data can be restored from backup media.
- ◆ Consider periodic audits by outside agencies to ensure that appropriate media controls are maintained.

Roadblocks

Unlike many business environments, there is no real control over movement of people and equipment on and off campus. While establishing controls for centrally managed data is relatively straightforward, the issue of enforcing media controls for “shadows” and other unofficial systems is a significant one.

Comments

A reasonable standard for purging magnetic media containing protected health information by overwriting is a one-time bit-by-bit method that wipes the entire piece of media. The government standard for declassifying media is a three-time overwrite: First overwrite with a

AMC/HIPAA Workgroup

character or character string, second overwrite with the binary compliment of the first, and the third overwrite may consist of any character or character string.

SEC.15 Physical access controls § .308(b)(3)

HIPAA Requirement

...(limited access) (formal, documented policies and procedures to be followed to limit physical access to an entity while ensuring that properly authorized access is allowed) that include all of the following implementation features:

(i) Disaster recovery (the process enabling an entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure).

(ii) An emergency mode operation (access controls in place that enable an entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure).

(iii) Equipment control (into and out of site) (documented security procedures for bringing hardware and software into and out of a facility and for maintaining a record of that equipment. This includes, but is not limited to, the marking, handling, and disposal of hardware and storage media.)

(iv) A facility security plan (a plan to safeguard the premises and building (exterior and interior) from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering, and theft).

(v) Procedures for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges)

(vi) Maintenance records (documentation of repairs and modifications to the physical components of a facility, such as hardware, software, walls, doors, and locks).

(vii) Need-to-know procedures for personnel access (a security principle stating that a user should have access only to the data he or she needs to perform a particular function).

(viii) Procedures to sign in visitors and provide escorts, if appropriate (formal documented procedure governing the reception and hosting of visitors).

(ix) Testing and revision (the restriction of program testing and revision to formally authorized personnel).

AMC Explanation of HIPAA Regulation

Each covered entity is required to establish formal, documented policies and procedures for limiting physical access while ensuring that properly authorized access is allowed. Mandatory implementation features also include plans for emergency operation and disaster recovery as well as for testing and revision.

Key Issues

None.

Category I Guidelines-Actions must be taken to address these

- ◆ House critical or sensitive protected health information processing facilities in secure areas, protected by a defined security perimeter, with appropriate security barriers and

AMC/HIPAA Workgroup

entry controls. Physically protect them from unauthorized access, damage, and interference.

- ◆ Establish and maintain a specific disaster recovery plan.
- ◆ Supervise or clear contractors and other visitors to secure areas, and record their date and time of entry and departure.
- ◆ Control access to protected health information and information processing facilities, and restrict it to authorized persons only.
- ◆ Provide security for off-site equipment that is equivalent to that provided for on-site equipment used for the same purpose, taking into account the risks of working outside the covered entity's premises.
- ◆ Keep records of maintenance of equipment.
- ◆ Restrict testing and revision to authorized personnel.

Category II Guidelines-Action should be considered to address these

- ◆ Provide protection commensurate with the identified risks.
- ◆ Regularly review and update access rights to secure areas.
- ◆ Grant contractors and visitors access only for specific, authorized purposes and issue them with instructions on the security requirements of the area and on emergency procedures.
- ◆ Require all workforce members to wear some form of visible identification and encourage them to challenge unescorted strangers and anyone not wearing visible identification.
- ◆ Physically protect equipment from security threats and environmental hazards.
- ◆ Maintain equipment in accordance with the supplier's recommended service intervals and specifications.
- ◆ Use authentication controls, e.g. swipe card plus PIN, to authorize and validate all access. Maintain a secure audit trail of all access.
- ◆ Require management authorization for the use of any equipment outside a covered entity's premises for processing of protected health information.
- ◆ Ensure that only authorized maintenance personnel carry out repairs and service equipment.
- ◆ Maintain records of all suspected or actual faults and all preventative and corrective maintenance.
- ◆ Establish appropriate controls when sending equipment off premises for maintenance.
- ◆ Comply with all requirements imposed by insurance policies.
- ◆ Check all items of equipment containing storage media, e.g. fixed hard disks, to ensure that any protected health information and licensed software has been removed or overwritten prior to disposal.
- ◆ Require authorization in order to take any equipment, protected health information, or software off site. Where necessary and appropriate, require equipment to be logged out and logged back in when returned. Perform spot checks to detect unauthorized removal of property, and make individuals aware that spot checks will take place.
- ◆ Forbid users to connect unauthorized devices to the enterprise network.
- ◆ Escort and supervise maintenance personnel; assign knowledgeable persons to this task.

AMC/HIPAA Workgroup

Roadblocks

Those responsible for implementation and enforcement may be slow to accept the need for new policies.

Comments

Also see: SEC.14 Media Controls

AMC/HIPAA Workgroup

SEC.16 Policy/guideline on workstation use § .308(b)(4)

HIPAA Requirement

...(documented instructions/procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific computer terminal site or type of site, dependent upon the sensitivity of the information accessed from that site).

AMC Explanation of HIPAA Regulation

Each covered entity is required to establish a policy/guideline on secure workstation use. These documents will establish the rules for minimizing the risk of exposing protected health information to unauthorized access. They will include technical measures (automatic logoff) as well as behavioral rules (no sharing of passwords).

Key Issues

- ◆ Is there a documented procedure for siting workstations (including both printers and data entry/display terminals) in such a way as to minimize shoulder surfing?
- ◆ Is there a process for determining automatic logoff intervals for each site?
- ◆ Is there a process for activating and deactivating passwords?
- ◆ Is there a documented process to train users about their responsibilities in maintaining workstation security?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop a Workstation Use Policy.
- ◆ Position workstations to minimize unauthorized viewing of protected health information either by shoulder surfing or by other direct physical means of obtaining access to data present on the workstation.
- ◆ Grant workstation access only to those who need it in order to perform their job function.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop a policy/guideline to protect the workstations from exposure to physical threats including theft.
- ◆ Consider establishing automatic logoff to minimize opportunities for unauthorized use of a workstation.
- ◆ Educate users about their responsibilities for workstation security.
- ◆ Monitor workstation sites for good user practice including logoff and password usage.
- ◆ Consider two-factor login for user authentication.
- ◆ Avoid login methods that may require the use of multiple passwords by an individual.

Roadblocks

In many institutions, guarding passwords and workstations is of secondary importance to the need to accomplish the goal of providing healthcare. Procedures that substantially impede the use of data entry and data retrieval will meet resistance.

AMC/HIPAA Workgroup

Comments

When interpreting this rule, consider that a workstation may include any or all of several devices such as data terminals, printers, and fax machines. Printouts may contain the most sensitive information in a patient's file and are as great a security risk as any other source of information. Since turnover may be high among those who have broad access to protected health information, it is important to have a facile and flexible way to manage granting and revocation of access privileges.

Training users about their security responsibilities as well as functional aspects is vital, especially in AMCs.

AMC/HIPAA Workgroup

SEC.17 Secure work station location § .308(b)(5)

HIPAA Requirement

...(physical safeguards to eliminate or minimize the possibility of unauthorized access to information; example, locating a terminal used to access sensitive information in a locked room and restricting access to that room authorized personnel, not placing terminal used to access patient information in any area of a doctor's office where the screen contents can viewed from the reception area).

AMC Explanation of HIPAA Regulation

Each covered entity is required to implement physical safeguards to eliminate or minimize the possibility of unauthorized access to protected health information. This is especially important in public buildings, provider locations, and other areas where there is heavy pedestrian traffic.

Key Issues

- ◆ What are the trade-offs between workstation accessibility and protection of protected health information?
- ◆ How will potential workstation location changes impact workflow?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected health information.
- ◆ Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to protected health information.

Category II Guidelines-Actions should be taken to address these

- ◆ When practical, locate workstations used to access protected health information in areas that are continuously monitored by cleared personnel when open for business and otherwise securely locked and alarmed with a 24 hour security monitoring service.
- ◆ Locate workstations to minimize the possibility of unauthorized personnel viewing screens or data.
- ◆ Establish workstation inactivity timeouts and use timed, password-protected screen savers.
- ◆ Consider the use of proximity detectors to reduce exposure at unattended workstations.

Roadblocks

No roadblocks specific to this point.

Comments

Ideally, workstations used to access protected health information would be located only in controlled areas — but this may unacceptably restrict access to and use of electronic patient records. In these cases, consider additional controls such physical devices to limit viewing,

AMC/HIPAA Workgroup

timeout/lockout of individual sessions, use of password-protected screensavers, and other procedures to provide adequate confidentiality.

SEC.18 Security Awareness training § .308(b)(6)

HIPAA Requirement

...(information security awareness training programs in which all employees, agents, and contractors must participate, including, based on job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security).

AMC Explanation of HIPAA Regulation

Covered entities are required to establish security awareness training programs customized to individual job responsibilities. Training for all workforce members in the use of protected health information and its confidentiality and security is required.

Key Issues

- ◆ How will the covered entity tailor security awareness training to hundreds of separate roles?
- ◆ How will the covered entity merge privacy training (use of information) with security training to address this requirement?

Category I Guidelines-Actions must be taken to address these

- ◆ Provide job-specific security awareness training to all workforce members.
- ◆ Focus the training on use of protected health information (privacy) and security.

Category II Guidelines-Actions should be taken to address these

- ◆ Make this aspect of training a supervisory or departmental responsibility, as appropriate.
- ◆ Consider the security guidelines in this document—Category I and Category II Guidelines—and determine which pertain to each job class. Develop a training program to communicate them.

Roadblocks

Developing meaningful job-specific training programs in large organizations is difficult. Making supervisors responsible and accountable for training at this level is an approach that should maximize the likelihood of success.

Comments

Also see: SEC.12, as covered in §.308(a)(12). SEC.12 Security Training is general in nature, establishing high-level expectations for all staff and somewhat more focused expectations for the system user community. This Security Awareness Training point focuses on customized education tailored to individual job responsibilities.

AMC/HIPAA Workgroup

Section Three: Requirements for Technical Security, Services, and Mechanisms

SEC.19 Access Control § .308(c)(1)(i)

HIPAA Requirement

The technical security services must include...Access control that includes:

(A) A procedure for emergency access (documented instructions for obtaining necessary information during a crisis) and

(B) At least one of the following implementation features:

1) context-based access (an access control procedure based on the context of a transaction as opposed to being based on attributes of the initiator or target)

2) role-based access

3) user-based access

(C) The optional use of encryption

AMC Explanation of HIPAA Regulation

Each covered entity is required to maintain a mechanism for access control that restricts access to resources and allows access only by privileged entities, providing access only to those workforce members with a business need for it. Possible types of access control include mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation. In addition, a mechanism to enable emergency access is required.

Key Issues

- ◆ Is there a documented procedure for emergency access?
- ◆ Is there a process for screening unwarranted demands for access?
- ◆ Do systems and applications have technical capability to implement user, role, or context-based access?
- ◆ Do systems prohibit or allow simultaneous access of the same user id/concurrent connections? Why or why not?
- ◆ Does the organization allow group, shared, trusted, or generic logon?
- ◆ How does encryption impact access control?

Category I Guidelines-Actions must be taken to address these

- ◆ Define a context-based, role-based, and/or user-based access policy as appropriate for each of the various situations in the covered entity and adopt implementation procedures to enforce need-to-know accordingly.
- ◆ Enact a clearly stated and widely understood “break the glass” procedure for allowing access via alternate and/or manual methods in the event of an emergency requiring access to protected health information.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish a centrally administered service to define access profiles—context-based, role-based, or user-based—and oversee consistent implementation of access control mechanisms.
- ◆ Document and test the emergency access procedure.

AMC/HIPAA Workgroup

- ◆ Evaluate information technology projects, proposals, contracts, and existing services for access control features and implementation.
- ◆ Consider adopting ASTM-defined healthcare roles.

Roadblocks

Centrally administered access control services are difficult to implement in the diverse IT environments typical of Academic Medical Centers. Take into consideration that reduced logon solutions, PKI, Kerberos, password brokering services, and the like are expensive, complicated, and often require expertise not found in the healthcare industry. Testing emergency access procedures in a realistic fashion is often cumbersome. Controlling contractor and business partner access is challenging, particularly when remote network connections are involved and accountability is necessary on the remote end. Modifying access profiles when staff change roles within the covered entity will require efficient communication between personnel and IT.

Comments

Also see: SEC.05 Information Access and Control, SEC.10 Security Management Process, and SEC.11 Termination Procedures

A user-based access model would require the organization to determine appropriate access for each individual user. A role-based access model would require the organization to develop an access profile for each role; for example, nurses, doctors, and desk attendants each have different access needs dependent upon their role in the organization. A context-based access model would, for example, allow all staff working in Endocrinology to access Endocrinology records. Some AMCs may choose to implement combinations of access models.

SEC.20 Audit Controls § .308(c)(1)(ii)

HIPAA Requirement

The technical security services must include...(mechanisms employed to record and examine system activity).

AMC Explanation of HIPAA Regulation

System activity logging is required in order to recreate pertinent system events and actions taken by system users and administrators. An audit process of examining logged information is required in order to identify questionable data access activities, investigate breaches, respond to potential weaknesses, and assess the security program.

Key Issues

- ◆ What activities need to be monitored?
- ◆ What level of logging detail is necessary?
- ◆ How long should covered entities retain audit log data?
- ◆ How should covered entities protect audit log data?
- ◆ Who may access audit log data?
- ◆ How can a covered entity identify inappropriate access?
- ◆ How can a covered entity best use audit tools to assess its security program?
- ◆ When should prospective audits be used?

Category I Guidelines-Actions must be taken to address these

- ◆ Employ event logging on systems that process or store protected health information where warranted by risk analysis.

Category II Guidelines-Actions should be taken to address these

- ◆ Log system administration events:
 - ▶ Creation and removal of accounts;
 - ▶ Assigning and changing of privileges;
 - ▶ Installation, maintenance, and changing of software;
 - ▶ Changes in hardware configurations.
- ◆ Log user activities:
 - ▶ Logon and logoff, both successful and unsuccessful;
 - ▶ Read, write, create, and delete actions at the file level;
 - ▶ Individual user access to individual patient records;
 - ▶ Attempts to access unauthorized data and/or services.
- ◆ Perform prospective audits of user activity where risk levels warrant.
- ◆ Maintain log data for a specified period of time.
- ◆ Protect system logs, especially those containing personally identifiable healthcare information, from unauthorized access or alteration.
- ◆ Employ audit reduction tools and/or “intelligent” methods of correlating log data to detect unauthorized activity and reduce volumes to manageable size.

AMC/HIPAA Workgroup

Roadblocks

Be aware that system audit logs can quickly become voluminous and require additional maintenance time. Prospective auditing and determining appropriateness of access and actions taken is an expensive, time consuming, and difficult process.

Comments

The purpose of system event logging is to be able to recreate pertinent events should a security violation or compromise occur. Log data is typically examined reactively, when indications of unauthorized activity are reported. How entities interpret and respond to findings is a measure of compliance. Because prospective audits are onerous and usually require the input of clinicians to resolve need-to-know issues, they should be performed sparingly and with good cause in accordance with risk and threat levels as determined through the risk analysis process.

Enterprise systems are normally subject to audit controls. Departmental systems and those with limited numbers of users and lower functionality, such as laboratory systems or those that feed data up to enterprise systems, are normally not subject to audit controls unless the risk analysis process determines otherwise. The risk analysis process should consider track records of violations. Logging and audit strategies should reflect levels of abuse. Logging to a high level of detail, such as individual keystroke capture, is generally not necessary.

The required retention period for audit log data may vary. In general, at least several months of data are necessary to adequately investigate instances of inappropriate access. The National Industrial Security Program, which oversees the protection of U.S. government classified information, requires at least six months of log data. This may be a reasonable and defensible goal for Academic Medical Centers as well.

Also see: SEC.06 Internal Audit, SEC.09 Security Incident Procedures, PRIV.53 Complaints, and PRIV.54 Sanctions.

SEC.21 Authorization Control § .308 (c)(3)

HIPAA Requirement

...(the mechanism for obtaining consent for the use and disclosure of health information) that includes at least one of the following implementation features:

- (A) Role-based access
- (B) User-based access

AMC Explanation of HIPAA Regulation

Covered entities must implement a mechanism to authorize the privileged use of protected health information available via systems and applications. The mechanism must limit these privileges to the maximum practical extent commensurate with professional needs.

Key Issues

- ◆ How can a covered entity determine which type of authorization mechanism—role-based or user-based—is appropriate?

Category I Guidelines-Actions must be taken to address these

- ◆ Employ a system or application-based mechanism to authorize activities within system resources in accordance with the Least Privilege Principle. (See Comments.)
- ◆ Implement:
 - ▶ A role-based mechanism where users with common information needs are provided access and privileges through common security authorization classes; or
 - ▶ A user-based mechanism where users' information access and privilege needs are determined and provided on an individual basis.
- ◆ Maintain individual accountability for actions taken by forbidding group (shared, generic, trusted, etc.) logons.

Category II Guidelines-Actions should be taken to address these

None.

Roadblocks

Implementing a data stewardship model is prudent but will likely be difficult in large covered entities. Individuals or groups sometimes perform stewardship functions but may not understand the concept of accountability for usage and disclosure.

Comments

The Least Privilege Principle pertains to one's ability to perform specified system functions. Users should not have system capabilities not required of their positions. For example, a user who requires only read access to medical information should not have the ability to change or delete it. AMCs will almost certainly use the role-based authorization approach given the large numbers of users typical of these organizations. Covered entities are cautioned to avoid developing too many authorization profiles in a role-based model, as management of a large number of profiles is unwieldy.

SEC.22 Data Authentication § .308 (c)(4)

HIPAA Requirement

...(The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.)

AMC Explanation of HIPAA Regulation

Each covered entity must be able to provide corroboration that protected health information in its possession has not been altered or destroyed in an unauthorized manner. Data corroboration methods include, but are not limited to, the use of checksums, double keying, message authentication codes, and digital signatures.

Key Issues

- ◆ Is the use of digital signatures a cost effective approach?
- ◆ Are technical integrity controls a reasonable expectation for more than certain critical functions?
- ◆ Can trusted procedures supplant technical controls in some respects?

Category I Guidelines-Actions must be taken to address these

- ◆ Employ technical controls such as checksums, digital signatures, double keying, and message authentication codes where feasible and appropriate to the level of risk.

Category II Guidelines-Actions should be taken to address these

- ◆ Employ technical integrity controls for critical automated functions such as physicians' orders and prescriptions.
- ◆ Procedural aspects closely related to technical authentication and integrity:
 - ▶ Maintain separation of duties. Avoid overlapping responsibilities of application and system programmers, data center operators, data base administrators, network operations, and user functions.
 - ▶ Establish and demonstrate change management discipline.

Roadblocks

No roadblocks specific to this point.

Comments

None.

SEC.23 Entity Authentication § .308 (c)(5)

HIPAA Requirement

...(the corroboration that an entity is the one claimed) that includes:

(A) Automatic logoff (a security procedure that causes an electronic session to terminate after a predetermined time of inactivity, such as 15 minutes), and
(B) Unique user identifier (a combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity).

(C) At least one of the following implementation features:

(1) Biometric identification (an identification system that identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and handwritten signature)).

(2) Password.

(3) Personal identification number (PIN) (a number or code assigned to an individual and used to provide verification of identity).

(4) A telephone callback procedure (method of authenticating the identity of the receiver and sender of information through a series of “questions” and “answers” sent back and forth establishing the identity of each). For example, when the communicating systems exchange a series of identification codes as part of the initiation of a session to exchange information, or when a host computer disconnects the initial session before the authentication is complete, and the host calls the user back to establish a session at a predetermined telephone number.

(5) Token.

AMC Explanation of HIPAA Regulation

Entities (an entity may be a person, system, or process) must be authenticated prior to accessing protected health information. Authentication is the process of corroborating that an entity is who or what it claims to be; it may occur through a trusted process such as the provision of a secret password, a personal identification number, or a token. Dial-up remote access users are subject to stronger, or two-tiered, authentication that may include telephone call-back or other strong authentication methods. Automatic log offs, or inactivity time-outs, can help enforce authentication by precluding others from accessing unattended sessions.

Key Issues

- ◆ Is a unique user ID with password authentication secure enough?
- ◆ Should alternative authentication methods such as biometrics be considered?
- ◆ What standards are necessary to make a public key infrastructure (PKI) interoperable and truly useful?

Category I Guidelines-Actions must be taken to address these

- ◆ Uniquely identify each user and authenticate identity.
- ◆ Implement at least one of the following methods to authenticate a user:

AMC/HIPAA Workgroup

- ▶ Password;
- ▶ Biometrics;
- ▶ Personal Identification Number (PIN);
- ▶ Physical token;
- ▶ Call-back or strong authentication for dial-up remote access users.
- ◆ Implement automatic log-offs to terminate sessions after set periods of inactivity. Determine appropriate periods based on the levels of risk and exposure.

Category II Guidelines-Actions should be taken to address these

- ◆ Include procedures for initiating user access, resetting passwords/tokens, and providing administrative access in the authentication system, and ensure it is fully documented.
- ◆ Employ a formal risk management methodology to identify risks and threats to the authentication process.
- ◆ Employ secure architectures, where risk appropriate, to authenticate entities. These may include Kerberos, RADIUS, TACACS, PKI, or similar methods.
- ◆ Encrypt hard-coded passwords that reside on client machines or in applications.
- ◆ Securely authenticate contractors. Device-to-device or firewall-to-firewall authentication is acceptable provided the contractor demonstrates individual accountability for access.
- ◆ Change passwords periodically.
- ◆ Specify time-out intervals based on business need and levels of risk and exposure.
- ◆ Allow users to select and change their own passwords.

Roadblocks

No roadblocks specific to this point.

Comments

Dial-back has been largely replaced by more robust architectures such as Remote Dial-In User Authentication (RADIUS). Most covered entities will continue to employ user ID and password authentication. Managed properly this is adequate, but processing speeds and wide availability of hacker tools and techniques have made this method obsolete for all but internal authentication. Inactivity time-outs are secondary controls and users should not rely on them to end their sessions. Password standards must be risk appropriate. Covered entities will need to address password length, complexity, change frequency, user selection, etc. This will continue to be a moving target.

SEC.24 Communications/network controls § .308(d)

HIPAA Requirement

- (1) If an entity uses communications or network controls, its security standards for technical security mechanisms must include the following:
- (i) The following implementation features:
 - (A) Integrity controls (a security mechanism employed to ensure the validity of the information being electronically transmitted or stored).
 - (B) Message authentication (ensuring, typically with a message authentication code, that a message received (usually via a network) matches the message sent).
 - (ii) One of the following implementation features:
 - (A) Access controls (protection of sensitive communications transmissions over open or private networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient).
 - (B) Encryption.
- (2) If an entity uses network controls (to protect sensitive communication that is transmitted electronically over open networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient), its technical security mechanisms must include all of the following implementation features:
- (i) Alarm. (In communication systems, any device that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. The signal may be in any desired form ranging from a simple contact closure (or opening) to a time-phased automatic shutdown and restart cycle.)
 - (ii) Audit trail (the data collected and potentially used to facilitate a security audit).
 - (iii) Entity authentication (a communications or network mechanism to irrefutably identify authorized users, programs, and processes and to deny access to unauthorized users, programs, and processes).
 - (iv) Event reporting (a network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information).

AMC Explanation of HIPAA Regulation

Covered entities that use external communication systems, such as the public switched telephone system, or open networks, such as the Internet, are required to safeguard protected health information that traverses them. The specified technical security services address network risks of message interception and interpretation by parties other than the intended recipient. Additionally, these services protect information systems from intruders attempting to exploit external communication points such as Internet host systems and telephone switches. In addition to the other listed precautions, some form of encryption is required when using open networks.

Key Issues

- ◆ How is relative risk determined?

AMC/HIPAA Workgroup

- ◆ How much encryption is enough?
- ◆ When should encryption be used?

Category I Guidelines-Actions must be taken to address these

- ◆ If the covered entity employs an internal, private, or value-added network, the covered entity must:
 - ▶ Employ alarms to sense abnormal conditions;
 - ▶ Enact an audit trail to recreate events in the instance of violations or compromises;
 - ▶ Identify and authenticate authorized users, programs, and processes;
 - ▶ Deny access to unauthorized users, programs, and processes;
 - ▶ Employ event reporting to identify operational irregularities and occurrences of significant tasks.
- ◆ If the covered entity employs the public switched telephone system, the covered entity must:
 - ▶ Enact integrity controls to ensure the validity of protected health information transmitted;
 - ▶ Enact message authentication to ensure that content is not altered in transmission;
 - ▶ Enact access controls or risk appropriate encryption to preclude unauthorized access, interception, or interpretation.
- ◆ If the covered entity employs the public Internet, the covered entity must enact the controls listed for the public switched telephone system as well as using risk appropriate encryption. (See Comments.)

Category II Guidelines-Actions should be taken to address these

- ◆ Do not store or transmit system passwords in the clear.
- ◆ Control network access through individual identification and authentication.
- ◆ Employ encryption keys of the length specified by the HCFA Internet Security Policy.

Roadblocks

Encryption is often difficult to implement. Hardware-based encryption is generally costly but fast because it does not require CPU cycles, while software-based encryption is generally less costly but tends to be system or application dependent and impedes performance.

Comments

Threats to data transmissions are difficult to quantify and widely misunderstood. Threat levels vary and are sometimes based on factors such as geography. For example, the threat of eavesdropping on the public switched telephone system within the United States is very low, but the threat rises dramatically when international communications are considered. State-sponsored eavesdropping is the norm in some parts of the world—particularly when U.S. interests are involved.

In November of 1998, the Healthcare Finance Administration (HCFA) released an Internet Security Policy describing appropriate encryption key lengths for public, private, and elliptical

AMC/HIPAA Workgroup

curve algorithms. Required key lengths are, of course, subject to change as technology improves. Academic Medical Centers should use strong encryption with key lengths at least as long as those specified by HCFA for Internet transmissions.

AMCs may need further advice from communications experts and national agencies/organizations.

AMC/HIPAA Workgroup

AMC HIPAA Privacy Guidelines

This part provides AMC guidelines for the use and disclosure of protected health information in accordance with the DHHS Final Privacy Rule [45 CFR 160]. The standards have been reorganized from the order that they appear in the rule in order to combine like topics into congruent sections, and in some cases to allow one guideline to address multiple standards where appropriate. Hopefully, the reorganization will be useful for covered entities seeking to implement and understand the relationship among the various standards. Guidelines are consolidated into sections as follows:

- ◆ Section One addresses guidelines involving covered entities (PRIV.01-PRIV.06).
- ◆ Section Two addresses guidelines for consent and authorization (PRIV.07-PRIV.12).
- ◆ Section Three addresses uses and disclosures (PRIV.13-PRIV.42).
- ◆ Section Four addresses consumer controls (PRIV.43-PRIV.47)
- ◆ Section Five addresses administrative requirements (PRIV.48-PRIV.59)

Table 1, Mapping of Privacy Standards to AMC Guidelines, provides a lookup table mapping each privacy standard to the corresponding AMC guideline.

Table 1. Mapping of Privacy Standards to AMC Guidelines

Privacy Rule	Standard	AMC Guideline
§164.502 (a)	Uses and disclosures	PRIV.13
§164.506 (e)	Resolving conflicting consents and authorizations	PRIV.08
§164.506 (f)	Joint consents	PRIV.09
§164.502 (b)	Minimum necessary	PRIV.39
§164.502 (c)	Uses and disclosures of protected health information subject to an agreed-upon restriction	PRIV.14
§164.502 (d)	Uses and disclosures of de-identified protected health information	PRIV.15
§164.502 (e)	Disclosures to business associates	PRIV.16
§164.502 (f)	Deceased individuals	PRIV.17
§164.502 (g)	Personal representatives	PRIV.18

AMC/HIPAA Workgroup

Privacy Rule	Standard	AMC Guideline
§164.502 (h)	Confidential communications	PRIV.19
§164.502 (i)	Uses and disclosures consistent with notice	PRIV.20
§164.502 (j)	Disclosures by whistleblowers and workforce member crime victims	PRIV.21
§164.504 (b)	Health care component	PRIV.01
§164.504 (d)	Affiliated covered entities	PRIV.02
§164.504 (e)(1)	Business associate contracts	PRIV.03
§164.504 (f)(1)	Requirements for group health plans	PRIV.04
§164.504 (g)	Requirements for a covered entity with multiple covered functions	PRIV.05
§164.506 (a)	Consent requirement	PRIV.07
§164.506 (e)	Resolving conflicting consents and authorizations	PRIV.08
§164.508 (a)	Authorizations for uses and disclosures	PRIV.10
§164.510 (a)	Use and disclosure for facility directories	PRIV.22
§164.510 (b)	Uses and disclosures for involvement in the individual's care and notification purposes	PRIV.23
§164.512 (a)	Uses and disclosures required by law	PRIV.27
§164.512 (b)	Uses and disclosures for public health activities	PRIV.28
§164.512 (c)	Disclosures about victims of abuse, neglect or domestic violence	PRIV.29
§164.512 (d)	Uses and disclosures for health oversight activities	PRIV.30
§164.512 (e)	Disclosures for judicial and administrative proceedings	PRIV.31

AMC/HIPAA Workgroup

Privacy Rule	Standard	AMC Guideline
§164.512 (f)	Disclosures for law enforcement purposes	PRIV.32
§164.512 (g)	Uses and disclosures about decedents	PRIV.33
§164.512 (h)	Uses and disclosures for cadaveric organ, eye, or tissue donation purposes	PRIV.34
§164.512 (i)	Uses and disclosures for research purposes	PRIV.35
§164.512 (j)	Uses and disclosures to avert a serious threat to health or safety	PRIV.36
§164.512 (k)	Uses and disclosures for specialized government functions	PRIV.37
§164.512 (l)	Disclosures for workers' compensation	PRIV.38
§164.514 (a and b)	De-identification of protected health information	PRIV.40
§164.514 (d)(1)	Minimum necessary requirements	PRIV.41
§164.514 (e)(1)	Uses and disclosures of protected health information for marketing	PRIV.24
§164.514 (f)(1)	Uses and disclosures for fund-raising	PRIV.25
§164.514 (g)	Uses and disclosures for underwriting and related purposes	PRIV.26
§164.514 (h)(1)	Verification requirements	PRIV.42
§164.520 (a)	Notice of privacy practices	PRIV.43
§164.522 (a)(1)	Right of an individual to request restriction of uses and disclosures	PRIV.11
§164.522 (b)(1)	Confidential communications requirements	PRIV.44
§164.524 (a)	Access to protected health information	PRIV.45

AMC/HIPAA Workgroup

Privacy Rule	Standard	AMC Guideline
	information	
§164.526 (a)	Right to amend	PRIV.46
§164.528 (a)	Right to an accounting of disclosures of protected health information	PRIV.47
§164.530 (a)(1)(i)	Personnel designations	PRIV.48 (Privacy Official)
§164.530 (a)(1)(ii)	Personnel designations	PRIV.49 (Contact Person)
§164.530 (b)(1)	Training	PRIV.50
§164.530 (c)(1)	Safeguards	PRIV.51
§164.530 (d)(1)	Complaints to the covered entity	PRIV.52
§164.530 (e)(1)	Sanctions	PRIV.53
§164.530 (f)	Mitigation	PRIV.54
§164.530 (g)	Refraining from intimidating or retaliatory acts	PRIV.55
§164.530 (h)	Waiver of rights	PRIV.56
§164.530 (i)(1)	Policies and procedures	PRIV.57
§164.530 (i)(2)	Changes to policies or procedures	PRIV.58
§164.530 (j)	Documentation	PRIV.59
§164.530 (k)	Group health plans	PRIV.06
§164.532 (a)	Effect of prior consents and authorizations	PRIV.12

AMC/HIPAA Workgroup

Section One: Covered Entities

PRIV.01 Health care component §[164.504\(b\)](#)

HIPAA Requirement

Standard: health care component. If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.

(c)

(1) Implementation specification: application of other provisions. In applying a provision of this subpart, other than this section, to a hybrid entity:

(i) A reference in such provision to a “covered entity” refers to a health care component of the covered entity;

(ii) A reference in such provision to a “health plan,” “covered health care provider,” or “health care clearinghouse” refers to a health care component of the covered entity if such health care component performs the functions of a health plan, covered health care provider, or health care clearinghouse, as applicable; and

(iii) A reference in such provision to “protected health information” refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.

(2) Implementation specifications: safeguard requirements. The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:

(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(ii) A component that is described by paragraph (2)(i) of the definition of health care component in this section does not use or disclose protected health information that is within paragraph (2)(ii) of such definition for purposes of its activities other than those described by paragraph (2)(i) of such definition in a way prohibited by this subpart; and

(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member’s work for the health care component in a way prohibited by this subpart.

(3) Implementation specifications: responsibilities of the covered entity. A covered entity that is a hybrid entity has the following responsibilities:

(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply with this subpart.

(ii) The covered entity has the responsibility for complying with [§ 164.530\(i\)](#), pertaining to the implementation of policies and procedures to ensure compliance

AMC/HIPAA Workgroup

with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by [§ 164.530\(j\)](#).

AMC Explanation of HIPAA Regulation

A hybrid entity is a single legal entity that is a covered entity, but one where its covered functions are not its primary function. While the HIPAA Privacy regulations classify the entire hybrid entity as a covered entity, the HIPAA privacy information disclosure and use requirements apply only to the entity's healthcare components. The hybrid entity is responsible for designating which of its components are healthcare components, and for ensuring that those components comply with the HIPAA privacy requirements.

Healthcare components of an entity must treat non-healthcare components of the entity as separate entities for the purposes of disclosure of protected health information. Individuals who work for both a healthcare component and other components of the entity must adhere to the HIPAA privacy information disclosure and use requirements when handling any protected health information they encounter as part of their duties in the healthcare component.

Key Issues

- ◆ What are the components of your entity?
- ◆ Which components are healthcare components?
- ◆ Do any members of your workforce work for more than one component of your hybrid entity?

Category I Guidelines-Actions must be taken to address these

- ◆ If your entity is a hybrid entity, designate which components of your entity are healthcare components. Document this designation.
- ◆ Ensure that all healthcare components of your entity comply with HIPAA privacy requirements.
- ◆ Identify any individuals who work for both healthcare components and non-healthcare components of your entity and ensure that they treat protected health information in accordance with the HIPAA privacy requirements. Make sure this is done on a regular basis, as workforce members change jobs.

Category II Guidelines-Actions should be taken to address these

- ◆ Make specialized training available to help workforce members who work for both healthcare and non-healthcare components be aware of their responsibilities.

Roadblocks

No roadblocks specific to this point.

Comments

None.

PRIV.02 Affiliated covered entities §[164.504\(d\)](#)

HIPAA Requirement

(1) Standard: affiliated covered entities. Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.

(2) Implementation specifications: requirements for designation of an affiliated covered entity. (i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.

(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by [§ 164.530\(j\)](#). (3) Implementation specifications: safeguard requirements. An affiliated covered entity must ensure that:

(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and

(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.

AMC Explanation of HIPAA Regulation

Several legally separate covered entities under common ownership or control may combine to form a single affiliated covered entity for the purposes of compliance with HIPAA privacy. If such an affiliated covered entity is created, the affiliated entity becomes responsible for compliance of all of its subsidiary entities. The creation of an affiliated covered entity must be documented.

Key Issues

- ◆ Is your entity eligible for affiliation under this part of the regulation: does it consist of multiple legally independent entities under common ownership and control?

Category I Guidelines-Actions must be taken to address these

- ◆ If an affiliated entity is created, make sure to document its creation according to the requirements of §164.530(j).

Category II Guidelines-Actions should be taken to address these

- ◆ Consult your legal staff about whether the creation of an affiliated entity would be advantageous.

Roadblocks

No roadblocks specific to this point.

AMC/HIPAA Workgroup

Comments

None.

HIPAA Requirement

Standard: business associate contracts. (i) The contract or other arrangement between the covered entity and the business associate required by [§ 164.502\(e\)\(2\)](#) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) Implementation specifications: business associate contracts. A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract; (C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with [§ 164.524](#);

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with [§164.526](#);

(G) Make available the information required to provide an accounting of disclosures in accordance with [§ 164.528](#); (H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the

AMC/HIPAA Workgroup

covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. (3) Implementation specifications: other arrangements. (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.

(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section. (ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(4) Implementation specifications: other requirements for contracts and other arrangements. (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or (B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that

AMC/HIPAA Workgroup

it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and
(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

AMC Explanation of HIPAA Regulation

A covered entity is required to ensure that any business associates with whom it shares protected health information handle that information in compliance with the privacy regulations. Covered entities must execute agreements requiring their business associates (and all agents or subcontractors of those business associates) to handle protected health information in accordance with HIPAA privacy requirements, and to take remedial action if they become aware that a business associate is not fulfilling its obligations under such an agreement. The regulation requires that such agreements contain specific terms, including terms requiring that business associates and their agents report violations of the HIPAA privacy regulations to the covered entity.

Key Issues

- ◆ With which persons or organizations is the covered entity required to execute a Chain of Trust Agreement?
- ◆ How will security responsibilities and accountabilities be determined, drafted, and monitored?
- ◆ What procedure will be followed if another entity refuses to sign a chain of trust agreement?
- ◆ How will the risk of a breach of confidentiality or data integrity be distributed among parties?
- ◆ What sanctions, other than termination of an agreement, are *reasonable* to protect all parties?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop a Chain of Trust Agreement, which must include:
 - ▶ Signatures of contracting parties. The contracts can be free-standing, or can be incorporated into, or as an addendum to, another contract.
 - ▶ Contract start date, expiration date, and/or review date. A certification audit must be documented and attached to the agreement.
 - ▶ Definition of Terms and Conditions, which must include conditions for disclosure of protected health information, data rights of each party, and minimum levels of security to be maintained.
 - ▶ Procedures for reporting breaches within a designated time frame.
 - ▶ A method of recording breaches. Each party must be able to provide its incident log for periodic inspection and upon demand.
 - ▶ Penalties for non-compliance (intentional versus unintentional).
 - ▶ Procedures for the retention and/or destruction of data.
 - ▶ Language requiring that subcontractors to the contracting party comply with the requirements of HIPAA privacy, together with a mutually agreed method for monitoring such compliance.

AMC/HIPAA Workgroup

Category II Guidelines-Actions should be taken to address these

- ◆ Implement a method to identify all of your entity's contracts.
- ◆ Develop standard contract terms for HIPAA privacy business associate provisions.
- ◆ Incorporate HIPAA business associate terms into existing contracts as part of your contract renewal process.

Roadblocks

Insurance requirements or liquidated damage clauses that institutions might require for protection of a breach by a business partner may be cost-prohibitive for small business partners, but termination of the contract is not always an adequate remedy.

Comments

As part of a compliance program, business associates should warrant, and the AMC's purchasing department should confirm, that the trading partner is not excluded from participation in any government program. Contracts should also include a statement that the business associate warrants that any subcontractors or agents are not excluded from participation in any government programs.

The Chain of Trust Agreement in the Supplement includes language for both the proposed security and privacy rules, except for the third party beneficiary language.

AMC/HIPAA Workgroup

PRIV.04 Requirements for group health plans [§164.504\(f\)\(1\)](#)

HIPAA Requirement

Standard: requirements for group health plans.

(i) Except as provided under paragraph (f)(1)(ii) of this section or as otherwise authorized under [§ 164.508](#), a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and discloses of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(2) Implementation specifications: requirements for plan documents. The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with [§ 164.524](#);

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with [§ 164.526](#);

(G) Make available the information required to provide an accounting of disclosures in accordance with [§ 164.528](#);

AMC/HIPAA Workgroup

- (H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;*
- (I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and*
- (J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.*
- (iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:*
- (A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;*
- (B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and*
- (C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.*
- (3) Implementation specifications: uses and disclosures. A group health plan may:*
- (i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;*
- (ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;*
- (iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and*
- (iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.*

AMC Explanation of HIPAA Regulation

Group health plans may disclose summary health information to their sponsors for specific purposes. They may also disclose other protected health information to plan sponsors for specific purposes, but only after the group health plan's plan documents have been amended to

AMC/HIPAA Workgroup

require the plan sponsor to conform to the HIPAA privacy regulation's provisions. The purposes for which group health plans may disclose summary health information to their sponsors without requiring modifications to the plan documents are limited to obtaining premium bids for providing coverage under the plan, or modifying, amending, or terminating the plan.

Group health plan sponsors are required to make their internal practices, books, and other internal documents relating to their handling of protected health information obtained from group health plans available to the Secretary of HHS for the purpose of determining whether the entity is in compliance.

Key Issues

- ◆ Determine whether your entity is a group health plan sponsor.
- ◆ Determine whether your entity is a group health plan.
- ◆ Determine whether you receive any protected health information from a group health plan as a group health plan sponsor.
- ◆ If your entity is a group health plan, define what constitutes summary health information that will be provided to plan sponsors.

Category I Guidelines-Actions must be taken to address these

- ◆ A group health plan must amend its plan documents to:
 - ▶ Establish permitted and required uses and disclosures of protected health information by the plan sponsor;
 - ▶ Describe which workforce members of the plan sponsor will be given access to the group health plan's protected health information;
 - ▶ Restrict access to and use by these workforce members to the plan administration functions which the plan sponsor performs for the group health plan;
 - ▶ Provide a procedure for resolving issues of noncompliance.
- ◆ The group health plan's sponsor must agree to:
 - ▶ Not use or further disclose protected health information provided by the plan other than as permitted or required by the plan documents or required by law;
 - ▶ Ensure that its agents adhere to the same rules it adheres to;
 - ▶ Not use protected health information for employment-related actions and decisions;
 - ▶ Not use protected health information for any other benefit or employee benefit plan;
 - ▶ Report any improper uses or disclosures of protected health information to the group health plan.
- ◆ The group health plan's sponsor must make certain information available to the group health plan:
 - ▶ make protected health information available to the group health plan for purposes of supporting requests to the plan for access to or amendment of protected health information.
 - ▶ make history of disclosures by the plan sponsor available to the group health plan.
- ◆ The group health plan's sponsor must make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary of HHS for the purpose of determining whether it is in compliance.

AMC/HIPAA Workgroup

- ◆ The group health plan's sponsor must (if feasible) return or destroy protected health information when it is no longer needed.

Category II Guidelines-Actions should be taken to address these

- ◆ Pay special attention to the provisions prohibiting a group health plan sponsor from using protected health information obtained from a group health plan for any employment-related action or decision. Consider clearly documenting which protected health information has been obtained under this section.

Roadblocks

No roadblocks specific to this point.

Comments

Many AMCs sponsor group health plans in which their employees are enrolled and for which they serve as third-party payers.

AMC/HIPAA Workgroup

PRIV.05 Requirements for a covered entity with multiple covered functions § 164.504(g)

HIPAA Requirement

Standard: requirements for a covered entity with multiple covered functions.

(1) *A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.*

(2) *A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.*

AMC Explanation of HIPAA Regulation

A covered entity which combines multiple covered functions (that is, which performs functions of a health plan, a health provider, and a health care clearinghouse) must comply with the provisions of the HIPAA privacy regulations governing each covered function. Further, a covered entity which combines multiple covered functions must restrict its uses and disclosures of protected health information to those appropriate to the function or functions it performs for each particular individual.

Key Issues

- ◆ If your entity provides both health plan and healthcare provider services, are there individuals for whom you provide one service but not the other?

Category I Guidelines-Actions must be taken to address these

- ◆ Identify the individuals for whom you provide only health plan services or only healthcare provider services.
- ◆ For individuals for whom you provide only health plan services, limit your uses and disclosures of their protected health information to those permitted to a health plan by the regulation.
- ◆ For individuals for whom you provide only healthcare provider services, limit your uses and disclosures of their protected health information to those permitted to a healthcare provider by the regulation.

Category II Guidelines-Actions should be taken to address these

None.

Roadblocks

No roadblocks specific to this point.

AMC/HIPAA Workgroup

Comments

None.

AMC/HIPAA Workgroup

PRIV.06 Group health plans [§ 164.530\(k\)](#)

HIPAA Requirement

(1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in [§ 164.504\(a\)](#); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with [§ 164.504\(f\)](#).

AMC Explanation of HIPAA Regulation

If an entity is a group health plan which provides benefits solely through an insurance contract with a health insurer or HMO, and if the entity receives only summary health information and plan participation status information, then the entity is exempt from the provisions of the HIPAA privacy regulations.

Key Issues

None.

Category I Guidelines-Actions must be taken to address these

- ◆ Determine whether your entity is exempt under this section.

Category II Guidelines-Actions should be taken to address these

None.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

Section Two: Consent and Authorization

HIPAA Requirement

Standard:

(a) *consent requirement.*

(1) *Except as provided in paragraph (a)(2) or (a)(3) of this section, a covered health care provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.*

(2) *A covered health care provider may, without consent, use or disclose protected health information to carry out treatment, payment, or health care operations, if:*

(i) *The covered health care provider has an indirect treatment relationship with the individual; or*

(ii) *The covered health care provider created or received the protected health information in the course of providing health care to an individual who is an inmate.*

(3)

(i) *A covered health care provider may, without prior consent, use or disclose protected health information created or received under paragraph (a)(3)(i)(A)-(C) of this section to carry out treatment, payment, or health care operations:*

(A) *In emergency treatment situations, if the covered health care provider attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment;*

(B) *If the covered health care provider is required by law to treat the individual, and the covered health care provider attempts to obtain such consent but is unable to obtain such consent; or*

(C) *If a covered health care provider attempts to obtain such consent from the individual but is unable to obtain such consent due to substantial barriers to communicating with the individual, and the covered health care provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.*

(ii) *A covered health care provider that fails to obtain such consent in accordance with paragraph (a)(3)(i) of this section must document its attempt to obtain consent and the reason why consent was not obtained.*

(4) *If a covered entity is not required to obtain consent by paragraph (a)(1) of this section, it may obtain an individual's consent for the covered entity's own use or disclosure of protected health information to carry out treatment, payment, or health care operations, provided that such consent meets the requirements of this section.*

(5) *Except as provided in paragraph (f)(1) of this section, a consent obtained by a covered entity under this section is not effective to permit another covered entity to use or disclose protected health information.*

(b) *Implementation specifications: general requirements.*

AMC/HIPAA Workgroup

- (1) A covered health care provider may condition treatment on the provision by the individual of a consent under this section.
- (2) A health plan may condition enrollment in the health plan on the provision by the individual of a consent under this section sought in conjunction with such enrollment.
- (3) A consent under this section may not be combined in a single document with the notice required by [§ 164.520](#).
- (4)
 - (i) A consent for use or disclosure may be combined with other types of written legal permission from the individual (e.g., an informed consent for treatment or a consent to assignment of benefits), if the consent under this section:
 - (A) Is visually and organizationally separate from such other written legal permission; and
 - (B) Is separately signed by the individual and dated.
 - (ii) A consent for use or disclosure may be combined with a research authorization under [§ 164.508\(f\)](#).
- (5) An individual may revoke a consent under this section at any time, except to the extent that the covered entity has taken action in reliance thereon. Such revocation must be in writing.
- (6) A covered entity must document and retain any signed consent under this section as required by [§ 164.530\(j\)](#).
- (c) Implementation specifications: content requirements. A consent under this section must be in plain language and:
 - (1) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment, or health care operations;
 - (2) Refer the individual to the notice required by [§ 164.520](#) for a more complete description of such uses and disclosures and state that the individual has the right to review the notice prior to signing the consent;
 - (3) If the covered entity has reserved the right to change its privacy practices that are described in the notice in accordance with [§ 164.520\(b\)\(1\)\(v\)\(C\)](#), state that the terms of its notice may change and describe how the individual may obtain a revised notice;
 - (4) State that:
 - (i) The individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment, or health care operations;
 - (ii) The covered entity is not required to agree to requested restrictions; and
 - (iii) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;
 - (5) State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and
 - (6) Be signed by the individual and dated.
- (d) Implementation specifications: defective consents. There is no consent under this section, if the document submitted has any of the following defects:

AMC/HIPAA Workgroup

- (1) *The consent lacks an element required by paragraph (c) of this section, as applicable; or*
- (2) *The consent has been revoked in accordance with paragraph (b)(5) of this section.*

AMC Explanation of HIPAA Regulation

A covered entity must have written consent from an individual before using or disclosing the individual's protected health information for treatment, payment, and health care operations. It is worth noting that the way the term "consent" is used in the regulation is different from the way it has traditionally been used. As traditionally used, "general consent" has meant consent for treatment, as an agent for collecting funds, and for assignment of benefits. In the regulation, "consents" are for the use and disclosure of information in the pursuit of providing health care. Consent under the regulation expands the type of information that can be released.

Key Issues

- ◆ When and where will consent be secured from individuals?
- ◆ How can a covered entity make consent information available in each setting where it has contact with an individual?
- ◆ How and when will the entity inform individuals of the entity's Privacy Notice as required under §164.520?
- ◆ How will a covered entity decide when or whether to agree to an individual's request that it restrict use and disclosure of protected health information for treatment, payment, or health care operations?
- ◆ What is the process for an individual to request restrictions upon use and disclosure of protected health information, or to change his or her consents for use and disclosure?
- ◆ If a covered entity does agree to restrictions, how will it track the status of consent related to any specific protected health information?
- ◆ What will an entity do if an individual does not consent to use or disclosure of protected health information? (Refusing to provide treatment or permit enrollment in a health plan are valid responses to an individual's failure to provide consent.)
- ◆ What is the duration of a consent?
- ◆ How can a consent be revoked?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop a procedure and a consent form to secure written consent for use or disclosure of protected health information to carry out treatment, payment, and health care operations when an individual first presents himself or herself to the covered entity.
- ◆ If protected health information is used or disclosed for treatment, payment, or health care operations without consent in an emergency, or as required by law, or if consent could not be obtained because of barriers in communication, attempt to get consent as soon as possible. If consent cannot be obtained, document the effort to get consent and state the reason consent was not obtained.
- ◆ Determine what action the covered entity will take if an individual will not consent to use or disclosure of protected health information or treatment, payment, or health care operations.

AMC/HIPAA Workgroup

- ◆ Identify actions to be taken when an individual revokes his or her consent. (The covered entity must comply with the revocation, except to the extent that the covered entity has taken action in reliance upon the original consent.)
- ◆ Develop a procedure to document and retain an individual's signed consent.
- ◆ Adopt a standard form for consent requests that contains all necessary elements cited in §164.506(c), as follows:
 - ▶ is written in plain language;
 - ▶ informs the individual that protected health information may be used and disclosed for treatment, payment, or health care operations;
 - ▶ informs the individual that the covered entity may change its privacy practices as described in its privacy notice and tells the individual how to get a revised notice;
 - ▶ states that the individual has a right to request restrictions upon use and disclosure of protected health information for treatment, payment and health care operations; that the covered entity does not have to agree to requested restrictions; and that if the covered entity does agree to restrictions, the restrictions are binding.
- ◆ Prohibit the use or disclosure of protected health information for marketing, sale, fund raising, and health plan enrollment decisions, employment determinations, or disclosure to non-related divisions and employers unless patient authorization is secured under §164.508/PRIV.10.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider obtaining consent for use or disclosure of protected health information even when it is not required.
- ◆ Consider using a time and date stamp on consent forms to be sure the handling of patient information was appropriate at the time it was done.
- ◆ Consider having a single point for disclosure of all information from the covered entity, even if decisions to use or disclose are made elsewhere.
- ◆ Instruct the privacy official to work with legal staff to ensure that contracts and business associate agreements reflect appropriate concern for the privacy and security of patient information.
- ◆ Consult with legal counsel about the documentation needed to support use or disclosure of protected health information when the entity was unable to obtain consent.

Roadblocks

Meeting use and disclosure consent requirements may require major organizational and educational effort within an AMC. An AMC may need to “prove” after the fact that it did not inappropriately use or disclose information, which could require a central record keeping system to track consents for use and disclosure.

Comments

The covered entity should make sure its decision-makers have a clear understanding of the differences between consent and authorization and the appropriate use of each under the HIPAA privacy regulations.

See §164.520/PRIV.43, the requirement to have a notice of privacy practices.

PRIV.08 Resolving conflicting consents and authorizations § [164.506\(e\)](#)

HIPAA Requirement

(e) Standard: resolving conflicting consents and authorizations.

(1) If a covered entity has obtained a consent under this section and receives any other authorization or written legal permission from the individual for a disclosure of protected health information to carry out treatment, payment, or health care operations, the covered entity may disclose such protected health information only in accordance with the more restrictive consent, authorization, or other written legal permission from the individual.

(2) A covered entity may attempt to resolve a conflict between consent and an authorization or other written legal permission from the individual described in paragraph (e)(1) of this section by:

(i) Obtaining a new consent from the individual under this section for the disclosure to carry out treatment, payment, or health care operations; or

(ii) Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered entity must document the individual's preference and may only disclose protected health information in accordance with the individual's preference.

AMC Explanation of HIPAA Regulation

If a covered entity has more than one consent document for an individual, it must adhere to the most restrictive one. The covered entity should attempt to resolve any differences between documents providing for differing consent.

Key Issues

- ◆ Does the covered entity have a procedure for securing consents and agreeing to revocations so as to minimize consent conflicts and aid in resolving differences?
- ◆ How will a covered entity know if it has multiple consent documents for use and disclosure of protected health information for an individual?
- ◆ How can a covered entity track its consents for individuals?
- ◆ Who determines whether or not one consent is more restrictive than another?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop a procedure to determine whether more than one consent for use and disclosure of protected health information exists for an individual.
- ◆ If more than one consent exists, determine if any conflicts exist between them, and if conflicts exist adhere to the most restrictive.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop a procedure for securing consents that will minimize the number of consents from any one individual and thus reduce the incidence of conflicts.
- ◆ Consider developing a single standard consent form for use in all encounters with an individual, and changing it infrequently.

AMC/HIPAA Workgroup

- ◆ If a consent conflict exists, contact the individual to clarify his or her preference and either:
 - ▶ Obtain a new written consent for use and disclosure or other clarification in writing, indicating that this document supercedes all other consents; or
 - ▶ Communicate with the individual, obtain verbal clarification, and document the conversation; and
 - ▶ Either way, from this point on, only use or disclose protected health information for treatment, payment, or health care operations as clarified by this contact.

Roadblocks

Any covered entity with a decentralized system of consents will have problems with this provision.

Comments

Remember that restrictiveness, not signing date, is the deciding factor between consents. A covered entity should be careful not to assume that the consent with the most recent date is the one that it should follow unless the later consent form explicitly supercedes the earlier one.

This problem would be easier to deal with if consent forms were standardized among referring entities.

PRIV.09 Joint consents [§ 164.506\(f\)](#)

HIPAA Requirement

(1) *Standard: joint consents. Covered entities that participate in an organized health care arrangement and that have a joint notice under [§ 164.520\(d\)](#) may comply with this section by a joint consent.*

Implementation specifications: requirements for joint consents.

(i) *A joint consent must:*

(A) *Include the name or other specific identification of the covered entities, or classes of covered entities, to which the joint consent applies; and*

(B) *Meet the requirements of this section, except that the statements required by this section may be altered to reflect the fact that the consent covers more than one covered entity.*

(ii) *If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as practicable.*

AMC Explanation of HIPAA Regulation

Separate covered entities that have formally agreed to participate in an organized health care arrangement may use a joint consent form covering all of the entities to obtain consent to use and disclose protected health information for the purposes of treatment, payment, and health care operations.

Key Issues

- ◆ Who will determine whether the consent form conforms to the requirements of this standard?
- ◆ How will a reliable process be established to notify each of the entities in the joint arrangement of a revoked consent?
- ◆ How will a reliable process be established for each covered entity to act in accordance with the revoked consent?

Category I Guidelines-Actions must be taken to address these

Determine if the covered entity is eligible to, or wants to, participate in a joint consent with others. If so:

- ◆ Create a joint consent form that meets the requirements of this standard:
 - ▶ Include on the joint consent form the individual names of each organization in the joint organization;
 - ▶ Include the other requirements of consent forms as specified in § 164.506(a).
- ◆ Establish a process for revocation of consent.
- ◆ Establish a process to notify each covered entity in the joint arrangement of revoked consents.
- ◆ Develop and use a joint notice of privacy practices.

AMC/HIPAA Workgroup

Category II Guidelines-Actions should be taken to address these

- ◆ Establish a process to recognize which individuals have no consent or have revoked consent for the use or disclosure of their protected health information for the purpose of treatment, payment, or health care operations.
- ◆ Establish a procedure that protects the protected health information of individuals with a revoked consent from use or disclosure.

Roadblocks

Tracking joint consents and revocations with multiple systems in different entities will be a difficult task.

Comments

Reference (§ 164.506(a).)/PRIV.07 and the section on notice of privacy practices §164.520(a)/PRIV.43.

It is not certain whether the existence of a more restrictive consent form for one of the entities would affect the responsibilities of other entities in the joint arrangement.

PRIV.10 Authorizations for uses and disclosures [§ 164.508\(a\)](#)

HIPAA Requirement

Standard: authorizations for uses and disclosures.

(1) *Authorization required: general rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.*

(2) *Authorization required: psychotherapy notes. Notwithstanding any other provision of this subpart, other than transition provisions provided for in [§ 164.532](#), a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:*

(i) *To carry out the following treatment, payment, or health care operations, consistent with consent requirements in [§ 164.506](#):*

(A) *Use by originator of the psychotherapy notes for treatment;*

(B) *Use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or*

(C) *Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual; and*

(ii) *A use or disclosure that is required by [§ 164.502\(a\)\(2\)\(ii\)](#) or permitted by [§ 164.512\(a\)](#); [§ 164.512\(d\)](#) with respect to the oversight of the originator of the psychotherapy notes; [§ 164.512\(g\)\(1\)](#); or [§ 164.512\(j\)\(1\)\(i\)](#).*

(b) *Implementation specifications: general requirements.*

(1) *Valid authorizations.*

(i) *A valid authorization is a document that contains the elements listed in paragraph (c) and, as applicable, paragraph (d), (e), or (f) of this section.*

(ii) *A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not be inconsistent with the elements required by this section.*

(2) *Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects:*

(i) *The expiration date has passed or the expiration event is known by the covered entity to have occurred;*

(ii) *The authorization has not been filled out completely, with respect to an element described by paragraph (c), (d), (e), or (f) of this section, if applicable;*

(iii) *The authorization is known by the covered entity to have been revoked;*

(iv) *The authorization lacks an element required by paragraph (c), (d), (e), or (f) of this section, if applicable;*

(v) *The authorization violates paragraph (b)(3) of this section, if applicable;*

(vi) *Any material information in the authorization is known by the covered entity to be false.*

AMC/HIPAA Workgroup

- (3) *Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:*
- (i) *An authorization for the use or disclosure of protected health information created for research that includes treatment of the individual may be combined as permitted by [§ 164.506\(b\)\(4\)\(ii\)](#) or paragraph (f) of this section;*
 - (ii) *An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;*
 - (iii) *An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.*
- (4) *Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:*
- (i) *A covered health care provider may condition the provision of research-related treatment on provision of an authorization under paragraph (f) of this section;*
 - (ii) *A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:*
 - (A) *The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and*
 - (B) *The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section;*
 - (iii) *A health plan may condition payment of a claim for specified benefits on provision of an authorization under paragraph (e) of this section, if:*
 - (A) *The disclosure is necessary to determine payment of such claim; and*
 - (B) *The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and*
 - (iv) *A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.*
- (5) *Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:*
- (i) *The covered entity has taken action in reliance thereon; or*
 - (ii) *If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.*

AMC/HIPAA Workgroup

- (6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by [§ 164.530\(j\)](#).
- (c) *Implementation specifications: core elements and requirements.*
- (1) *Core elements.* A valid authorization under this section must contain at least the following elements:
- (i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
 - (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
 - (iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
 - (iv) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
 - (v) A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
 - (vi) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;
 - (vii) Signature of the individual and date; and
 - (viii) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.
- (2) *Plain language requirement.* The authorization must be written in plain language.
- (d) *Implementation specifications: authorizations requested by a covered entity for its own uses and disclosures.* If an authorization is requested by a covered entity for its own use or disclosure of protected health information that it maintains, the covered entity must comply with the following requirements.
- (1) *Required elements.* The authorization for the uses or disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:
- (i) For any authorization to which the prohibition on conditioning in paragraph (b)(4) of this section applies, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;
 - (ii) A description of each purpose of the requested use or disclosure;
 - (iii) A statement that the individual may:
 - (A) Inspect or copy the protected health information to be used or disclosed as provided in [§ 164.524](#); and
 - (B) Refuse to sign the authorization; and
 - (iv) If use or disclosure of the requested information will result in direct or indirect remuneration to the covered entity from a third party, a statement that such remuneration will result.
- (2) *Copy to the individual.* A covered entity must provide the individual with a copy of the signed authorization.

AMC/HIPAA Workgroup

- (e) *Implementation specifications: authorizations requested by a covered entity for disclosures by others. If an authorization is requested by a covered entity for another covered entity to disclose protected health information to the covered entity requesting the authorization to carry out treatment, payment, or health care operations, the covered entity requesting the authorization must comply with the following requirements.*
- (1) *Required elements. The authorization for the disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:*
- (i) *A description of each purpose of the requested disclosure;*
- (ii) *Except for an authorization on which payment may be conditioned under paragraph (b)(4)(iii) of this section, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure; and*
- (iii) *A statement that the individual may refuse to sign the authorization.*
- (2) *Copy to the individual. A covered entity must provide the individual with a copy of the signed authorization.*
- (f) *Implementation specifications: authorizations for uses and disclosures of protected health information created for research that includes treatment of the individual.*
- (1) *Required elements. Except as otherwise permitted by [§ 164.512\(i\)](#), a covered entity that creates protected health information for the purpose, in whole or in part, of research that includes treatment of individuals must obtain an authorization for the use or disclosure of such information. Such authorization must:*
- (i) *For uses and disclosures not otherwise permitted or required under this subpart, meet the requirements of paragraphs (c) and (d) of this section; and*
- (ii) *Contain:*
- (A) *A description of the extent to which such protected health information will be used or disclosed to carry out treatment, payment, or health care operations;*
- (B) *A description of any protected health information that will not be used or disclosed for purposes permitted in accordance with [§§ 164.510](#) and [164.512](#), provided that the covered entity may not include a limitation affecting its right to make a use or disclosure that is required by law or permitted by [§ 164.512\(j\)\(1\)\(i\)](#); and*
- (C) *If the covered entity has obtained or intends to obtain the individual's consent under [§ 164.506](#), or has provided or intends to provide the individual with a notice under [§ 164.520](#), the authorization must refer to that consent or notice, as applicable, and state that the statements made pursuant to this section are binding.*
- (2) *Optional procedure. An authorization under this paragraph may be in the same document as:*
- (i) *A consent to participate in the research;*
- (ii) *A consent to use or disclose protected health information to carry out treatment, payment, or health care operations under [§ 164.506](#); or*

AMC/HIPAA Workgroup

(iii) A notice of privacy practices under [§ 164.520](#).

AMC Explanation of HIPAA Regulation

Although this section is lengthy, the gist of the HIPAA requirement is that a covered entity must have written authorization from an individual before using or disclosing the patient's protected health information and that the individual has the right to revoke that authorization.

The usual exceptions of treatment, payment, and health care operations do not require authorization (but do require consent; see § 164.506). Neither is authorization required for uses and disclosures under §§ 164.510 and 164.522, for public health and health oversight, certain law enforcement requirements, to medical examiners, and required disclosure to the Secretary, and §§ 164.514(e) and 164.514(f) for marketing and fundraising. In AMCs, typical examples of uses that would require authorizations are research without an IRB waiver and special marketing or press events featuring patients.

Key Issues

- ◆ How will a covered entity track the status of an authorization related to any specific patient information?
- ◆ How will a covered entity determine expiration dates (or events) for an authorization?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop a clearly written and complete statement covering use and disclosure practices for the covered entity, and publish it in the privacy notice.
- ◆ Develop policies to document and retain any signed authorization.
- ◆ Ensure that policies are in place and are followed for authorizations for use and disclosure of protected health information for psychotherapy notes, for compound authorizations, and for treatment related to research.
- ◆ Adopt appropriate forms for use and disclosure authorizations that contains each of the core elements cited in the regulation as follows:
 - ▶ describes the information to be used or disclosed;
 - ▶ identifies the person authorized to make the requested use or disclosure;
 - ▶ identifies the person to whom the covered entity may make the requested use or disclosure;
 - ▶ includes an expiration date or an event that triggers expiration;
 - ▶ states that the individual has a right to revoke the authorization, with exceptions identified, and describes how revocation may be done;
 - ▶ includes the individual's signature and the date;
 - ▶ if signed by a personal representative, includes a description of the representative's authority;
 - ▶ is written in plain language.
- ◆ Develop policies to ensure that the individual is given a copy of each signed authorization requested by a covered entity for its own use and disclosure or for disclosures requested by others.

AMC/HIPAA Workgroup

- ◆ Prohibit use or disclosure of protected health information for sale, health plan enrollment decisions, and employment determinations, and prohibit disclosure to non-related divisions and employers unless appropriate patient authorization has been secured.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider having a single point for disclosure of all information from the covered entity, even if decisions to use or disclose are made elsewhere.
- ◆ Have the privacy official should work with legal staff to ensure that the covered entity's contracts and business partner agreements reflect appropriate concern for the privacy and security of patient information.
- ◆ Develop clearly understood use and disclosure guidelines for development and marketing functions.
- ◆ Consider defining a set of reasonably broad authorizations and developing the ability to track what the user has authorized.

Roadblocks

An AMC will likely need a central record keeping system to track authorizations for use and disclosure for the clinical enterprise, and to retain them in case they are needed in order to prove it did not inappropriately disclose information. The IRB may need additional resources to manage the authorizations for protected health information created for research.

Comments

An AMC should carefully consider how to incorporate HIPAA requirements into existing research efforts and not assume that all research use and disclosure will be covered by IRB requirements. The HIPAA requirements do add to the activities of the IRB for review of informed consent, particularly in the core elements (c)(iii), (vi), and (viii). Current IRB regulations allow for "verbal" informed consent in limited situations; verbal consent is not adequate under the HIPAA privacy regulations. A standard IRB informed consent can be used for the authorization for research provided that the additional elements required by HIPAA are included. Consider how these requirements might affect research that is unrelated to treatment, and how these requirements could be incorporated into clinical trials.

An AMC might need a time and date stamp on permissions and revocations to ensure that it can document that its handling of patient information was appropriate at the time it was done.

AMC/HIPAA Workgroup

PRIV.11 Right of an individual to request restriction of uses and disclosures § 164.522(a)(1)

HIPAA Requirement

Standard: right of an individual to request restriction of uses and disclosures.

(i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under [§ 164.510\(b\)](#).

(ii) A covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under [§§ 164.502\(a\)\(2\)\(i\)](#), [164.510\(a\)](#) or [164.512](#).

(2) Implementation specifications: terminating a restriction. A covered entity may terminate its agreement to a restriction, if :

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

(3) Implementation specification: documentation. A covered entity that agrees to a restriction must document the restriction in accordance with [§164.530\(j\)](#).

AMC Explanation of HIPAA Regulation

A covered entity must have a process to accept and respond to a patient's request for restrictions on uses and disclosures of his or her protected health information for treatment, payment, or health care operations. A covered entity is not, however, required to accede to such requests.

Key Issues

- ◆ Within the covered entity, who makes the decision about handling patient restriction requests?

AMC/HIPAA Workgroup

- ◆ Should covered entities attempt to comply with “reasonable” patient restriction requests or should they deny all requests?
- ◆ Who will be responsible for communicating restrictions on protected health information disclosed to providers for emergency care?
- ◆ Who will be responsible for implementing procedures that comply with this standard when the covered entity decides to terminate a restriction?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish a policy to allow or deny restrictions.
- ◆ Establish procedures for patients to request restrictions.
- ◆ Document any agreed-to restrictions.
- ◆ Establish a process to ensure communication of and compliance with any agreed-to restrictions.
- ◆ Notify others to whom restricted information is released of such restrictions.
- ◆ Establish a process to notify providers to whom protected health information has been disclosed for emergency care of any restrictions on use or disclosure that apply.
- ◆ Establish procedures for documenting and terminating a restriction for each of the following circumstances:
 - ▶ When an individual requests a termination in writing;
 - ▶ When an individual orally agrees to the termination;
 - ▶ When the covered entity informs the individual that it is terminating its agreement to a restriction.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop an integrated audit function to track protected health information covered by restriction requests.
- ◆ Develop consistent policies regarding the application of restrictions for any provider agreeing to restrictions.
- ◆ Maintain a comprehensive record of any agreed-to restrictions.
- ◆ Identify any agreed to restrictions within each affected patient’s record.

Road Blocks

AMCs may not currently have the technology or the administrative processes to comply with a wide range of restriction requests. Without fully integrated computer systems, complying with access restriction requests will be extremely difficult. A decentralized administrative or computer structure will make complying with access restriction requests even more difficult.

Comments

An AMC may want to consider notifying patients of the *known* exceptions to restrictions. A health care provider cannot agree to restrictions on disclosures that are required by the HIPAA regulations or other laws. (See §§ 164.502(a)(2)(i), 164.510(a) or 164.512.)

An AMC may also want to consider if denying patient restriction requests will ultimately have a negative impact on the provider. (Is this ultimately a *business* decision or a *health care* decision?)

PRIV.12 **Effect of prior consents and authorizations [§ 164.532\(a\)](#)**

HIPAA Requirement

Standard: effect of prior consents and authorizations. Notwithstanding other sections of this subpart, a covered entity may continue to use or disclose protected health information pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information that does not comply with [§§ 164.506](#) or [164.508](#) of this subpart consistent with paragraph (b) of this section.

(b) Implementation specification: requirements for retaining effectiveness of prior consents and authorizations. Notwithstanding other sections of this subpart, the information pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, if the consent, authorization, or other express legal permission was obtained from an individual before the applicable compliance date of this subpart and does not comply with [§§ 164.506](#) or [164.508](#) of this subpart.

(1) If the consent, authorization, or other express legal permission obtained from an individual permits a use or disclosure for purposes of carrying out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission obtained from an individual applies, use or disclose such information for purposes of carrying out treatment, payment, or health care operations, provided that: following provisions apply to use or disclosure by a covered entity of protected health

(i) The covered entity does may not make any use or disclosure that is expressly excluded from the a consent, authorization, or other express legal permission obtained from an individual; and

(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(2) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for a purpose other than to carry out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission obtained from an individual applies, make such use or disclosure, provided that:

(i) The covered entity does not make any use or disclosure that is expressly excluded from the consent, authorization, or other express legal permission obtained from an individual; and

(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

AMC/HIPAA Workgroup

(3) In the case of a consent, authorization, or other express legal permission obtained from an individual that identifies a specific research project that includes treatment of individuals:

(i) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for purposes of the project, the covered entity may, with respect to protected health information that it created or received either before or after the applicable compliance date of this subpart and to which the consent or authorization applies, make such use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(ii) If the consent, authorization, or other express legal permission obtained from an individual is a general consent to participate in the project, and a covered entity is conducting or participating in the research, such covered entity may, with respect to protected health information that it created or received as part of the project before or after the applicable compliance date of this subpart, make a use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(4) If, after the applicable compliance date of this subpart, a covered entity agrees to a restriction requested by an individual under [§ 164.522\(a\)](#), a subsequent use or disclosure of protected health information that is subject to the restriction based on a consent, authorization, or other express legal permission obtained from an individual as given effect by paragraph (b) of this section, must comply with such restriction.

AMC Explanation of HIPAA Regulation

Covered entities may continue to use prior consents, authorizations, and legal permissions for use and disclosure of protected health information *created prior to the HIPAA compliance date* for treatment, payment, health care operations, and other purposes. If the prior consent or authorization is in regard to a research project, the covered entity may use or disclose protected health information received or created either before or after the HIPAA compliance date for that purpose.

Key Issues

- ◆ How will a covered entity identify and track prior consents and authorizations for protected health information?
- ◆ How can a covered entity be sure of the date any specific protected health information was created or received?

Category I Guidelines-Actions must be taken to address these

- ◆ Decide whether or not to treat protected health information created or received before the HIPAA compliance date with a different set of privacy consents and authorizations from protected health information created or received after the HIPAA compliance date.

AMC/HIPAA Workgroup

- ◆ If protected health information will be handled in different ways depending on the date it was created or received, clearly identify the protected health information that existed before the HIPAA compliance date.
- ◆ Verify that uses and disclosures of protected health information are in accordance with the consent, authorization, or other documented wishes of the individual that were effective at the time the protected health information was created or received.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider using HIPAA standards for all uses and disclosures of protected health information, whether it was created before or after the HIPAA compliance date, once the HIPAA regulations are in effect.

Roadblocks

Keeping track of differing consents and authorizations for use and/or disclosure of protected health information will be difficult, as it will require the covered entity to treat protected health information with different standards depending upon its date of creation or receipt.

Comments

None.

AMC/HIPAA Workgroup

Section Three: Uses and disclosures

AMC/HIPAA Workgroup

Sub-Section A: General Uses and Disclosures

AMC/HIPAA Workgroup

PRIV.13 Uses and disclosures of protected health information [§ 164.502\(a\)](#)

HIPAA Requirement

Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

- (i) To the individual;
- (ii) Pursuant to and in compliance with a consent that complies with [§ 164.506](#), to carry out treatment, payment, or health care operations;
- (iii) Without consent, if consent is not required under § 164.506(a) and has not been sought under § 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes;
- (iv) Pursuant to and in compliance with an authorization that complies with [§ 164.508](#);
- (v) Pursuant to an agreement under, or as otherwise permitted by, [§ 164.510](#); and
- (vi) As permitted by and in compliance with this section, [§ 164.512](#), or [§ 164.514\(e\)](#), (f), and (g).

(2) Required disclosures. A covered entity is required to disclose protected health information:

- (i) To an individual, when requested under, and as required by [§§ 164.524](#) or [164.528](#); and
- (ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

AMC Explanation of HIPAA Regulation

This is a general provision identifying the conditional uses and disclosures of protected health information. Only uses and disclosures that are permitted or required by the regulations are allowed. (The reader should review the definitions of use and disclosure carefully.)

The *permitted* uses/disclosures are: (i) to the individual; (ii) with consent of the patient for treatment, payment, and health care operations, all of which are well defined terms in the regulations; (iii) without consent in limited cases for treatment, payment, and healthcare operations (e.g. inmates, emergencies – see PRIV.07 and § 164.506); (iv) with an authorization from the patient; (v) without written consent but with an opportunity to agree or disagree prior to the use or release (e.g. patient directory listing); and (vi) when data is de-identified or when the public good (as defined) permits the use/disclosure.

The only two *required* uses/disclosures are: (i) to the individual who is the subject of the records; and (ii) to HHS to investigate compliance with the regulations.

AMC/HIPAA Workgroup

Key Issues

- ◆ What effects on cost and operations will flow from various alternatives about how an AMC defines the “covered entity” or “covered entities,” i.e. as a component, hybrid, organized healthcare system, or simple entity? This choice will determine whether some activities are “uses” or “disclosures.”
- ◆ Are there any uses or disclosures currently performed without authorization that will require an authorization under the HIPAA privacy regulations (especially those that the patient may not agree to)?
- ◆ Should covered entities provide a central store of consents, authorizations, and revocations?
- ◆ How much new work will be created by the possible release of records (all records; not just what is now thought of as the medical record) to patients?
- ◆ Will de-identifying be used much more frequently under these regulations than it is now?

Category I Guidelines-Actions must be taken to address these

- ◆ The covered entity must limit its uses and disclosures to those permitted or required.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider managing the consents and authorizations centrally for each covered entity in the AMC.
- ◆ Consider obtaining compliant consents and authorizations prior to the effective date of the regulations.
- ◆ Examine and amend any programs for which patients may not currently give authorization to have their protected health information used or disclosed.
- ◆ Consider adapting existing procedures where only small changes are needed for compliance prior to starting new procedures in programs where no procedure currently exists.

Roadblocks

Achieving compliance is partially dependent on consistent practice and effective communication across AMC operational units. This effort will be challenging for most AMCs.

Comments

For most AMCs, developing procedures and documentation standards will be a significant undertaking. The decentralized nature of most AMCs will make the coordination of consents and authorizations challenging. A lack of coordination, however, will increase the risk of improper sharing of information across the covered entity. Even when managed properly, privacy is a personal thing and the perception of individual mistrust could be felt across the different operational units within an AMC.

This is an area in which some states have stricter law; such laws still apply under the HIPAA privacy regulations.

AMC/HIPAA Workgroup

PRIV.14 Uses and disclosures of protected health information subject to an agreed-upon restriction [§ 164.502\(c\)](#)

HIPAA Requirement

Standard: uses and disclosures of protected health information subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to [§ 164.522\(a\)\(1\)](#) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

AMC Explanation of HIPAA Regulation

This provision of the regulations requires covered entities that have agreed to a restriction on use or disclosure of an individual's protected health information to respect the agreed-to restrictions unless and until they are revoked. There is an exception for use or disclosure in emergency circumstances in § 164.522(a).

Key Issues

- ◆ How much complexity in operations and communications will be created by the use of different use/disclosure “policies” for different patients?
- ◆ Will some patients not participate well in treatment without special restrictions?
- ◆ Can record use/disclosure be satisfactorily restricted without running afoul of legal requirements to use/disclose protected health information?
- ◆ How will providers and others be kept aware of specific restrictions for specific patients over time as they change?
- ◆ How will pre-HIPAA restrictive agreements be treated?

Category I Guidelines-Actions must be taken to address these

- ◆ Abide by any restrictions the covered entity agrees to.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider the practicality of respecting a restriction prior to agreeing to it, and weigh that practicality against the willingness of the patient to participate fully in care without the restriction.
- ◆ Consider the most common causes for requests for special restrictions, and design a small set of restriction protocols to accommodate these common causes where practical (e.g., celebrity, social stigma, physical danger).
- ◆ Establish a systematic way of communicating restrictions to workforce members, some of whom may become workforce members after the restriction comes into being.
- ◆ Avoid making the totality of special restrictions for patients treated by the same workforce members too complex for the staff to respect all of them.
- ◆ When patients ask for restrictions that cannot be agreed to, the covered entity should, when possible, refer them to a facility that can honor the restriction.
- ◆ Examine existing programs for providing aliases for patients for use in complying with this provision.

AMC/HIPAA Workgroup

Roadblocks

The staff can only handle so much complexity of use/disclosure protocol. This limit may be short of what some patients would prefer.

Comments

AMCs treat people who have cause for special restrictions: celebrities, people with socially stigmatized diseases, people in physical danger if their information is improperly used or disclosed, and so on. Treating these people optimally may involve some restrictions that would be untenable or contrary to what other patients desire in their own cases.

In the special, though common, case of a member of the AMC workforce wanting restrictions that guarantee that colleagues and the employer do not have access to information about the workforce member's health status, there may be no way for the AMC to accommodate the individual's request short of referral to another facility.

AMC/HIPAA Workgroup

PRIV.15 Uses and disclosures of de-identified protected health information **§ 164.502(d)**

The complete description of the issues related to de-identification is in the section related to § 164.514(a), described below in PRIV.40.

HIPAA Requirement

Standard: uses and disclosures of de-identified protected health information.

(1) Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) Uses and disclosures of de-identified information. Health information that meets the standard and implementation specifications for de-identification under [§ 164.514\(a\)](#) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of r 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

HIPAA Requirement

(1) Standard: disclosures to business associates.

(i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of [§ 164.504\(f\)](#) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and [§ 164.504\(e\)](#).

(2) Implementation specification: documentation. A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of [§ 164.504\(e\)](#).

AMC Explanation of HIPAA Regulation

The scope of this point is captured in the phrase requiring the covered entity to “obtain[] satisfactory assurance that the business associate will appropriately safeguard the information.” The rest of the regulation text elaborates how to obtain and demonstrate this assurance. The key point in this elaboration is a set of contractual requirements that the covered entity must impose on a business associate whether the business associate is itself a covered entity or not. There are three exceptions: disclosures to health care providers for treatment; disclosures by a group health plan, insurance issuer, or HMO to the plan sponsor (which must instead follow [§ 164.504\(f\)](#)); and disclosures between two government agencies that are allowed by law to share certain data in the performance of a government health plan’s functions.

AMC/HIPAA Workgroup

Key Issues

- ◆ How many business associate relations will require new contractual language and processes to implement the provisions?
- ◆ How much variety in privacy-maintenance processes can one AMC or one business associate realistically implement among its (typically) several hundred business associates with whom it shares protected health information?
- ◆ How does the requirement for the covered entity to “mitigate harm” (see § 164.530(f)) when it knows of an inappropriate use or disclosure by a business associate affect the “indemnification” terms of the contract? Note that § 164.504(e) requires business associates to report known inappropriate uses or disclosures to the covered entity.
- ◆ How will this regulation change agreements with those business associates with whom a covered entity already has a confidentiality agreement (e.g. attorneys)?

Category I Guidelines-Actions must be taken to address these

- ◆ Covered entities must create and manage the contractual requirements as provided in this section.

Category II Guidelines-Actions should be taken to address these

- ◆ To improve efficiency, consider using terms that standardize the operational requirements on the covered entity and on its business associates.
- ◆ Consider encouraging the business associate community to use standard terms so it will have standardized operational requirements with all of the covered entities with which it contracts.
- ◆ Engage in a systematic process of review, amendment (or creation), and negotiation of contracts well before the effective date of the regulations.

Roadblocks

This point could lead to a profusion of contractual terms requiring a profusion of behaviors in each covered entity and business associate of covered entities. It is not yet apparent how and when more standardized terms that might induce simpler operations models will emerge; if they do emerge, it will likely have to be at the national level.

The timeframe to amend and negotiate the typically several hundred affected contracts in an AMC is likely too short, and the staff time necessary to handle this process will be challenging to find.

Comments

The HIPAA statute did not allow direct regulation of all entities creating/receiving protected health information. This provision exists to ensure that safeguards for handling of protected health information apply to business associates of covered entities, since the statute did not permit them to be directly regulated.

AMC/HIPAA Workgroup

PRIV.17 Deceased individuals [§ 164.502\(f\)](#)

The complete description of issues related to deceased individuals is in the section related to § 164.512(g) described below in PRIV.33.

HIPAA Requirement

Standard: deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.

HIPAA Requirement

- (1) *Standard: personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.*
- (2) *Implementation specification: adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.*
- (3) *Implementation specification: unemancipated minors. If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:*
 - (i) *The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;*
 - (ii) *The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service;*
or
 - (iii) *A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.*
- (4) *Implementation specification: deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.*
- (5) *Implementation specification: abuse, neglect, endangerment situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:*
 - (i) *The covered entity has a reasonable belief that:*
 - (A) *The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or*

AMC/HIPAA Workgroup

- (B) Treating such person as the personal representative could endanger the individual; and*
- (ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.*

AMC Explanation of HIPAA Regulation

This section describes the conditions of use for protected health information with respect to personal representatives.

Key Issues

- ◆ Who will determine who is the appropriate personal representative?
- ◆ How will the determination of the personal representative be documented and by whom?
- ◆ What needs to occur if an entity elects not to treat a person as the personal representative?
- ◆ What are the liabilities associated with denying someone as a personal representative because of abuse, neglect, or endangerment situations and later finding out one was wrong? How can a covered entity mitigate the risk?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop policy and procedures for determining who qualifies as a personal representative.

Category II Guidelines-Actions should be taken to address these

- ◆ The designated personal representative should be explicitly documented.
- ◆ The designated personal representative should be educated on his or her rights and responsibilities.

Roadblocks

No roadblocks specific to this point.

Comments

AMCs should work closely with their legal counsels on this provision. It will be important to consider and address legal issues when developing the policies and procedures.

AMC/HIPAA Workgroup

PRIV.19 Confidential communications [§ 164.502\(h\)](#)

The complete description of issues related to confidential communication is in the section related to § 164.522(b) described below in PRIV.44.

HIPAA Requirement

Standard: confidential communications. A covered health care provider or health plan must comply with the applicable requirements of [§ 164.522\(b\)](#) in communicating protected health information.

Section § 164.522(b):

(b)(1) Standard: confidential communications requirements.

(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual,

(2) Implementation specifications: conditions on providing confidential communications.

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

AMC/HIPAA Workgroup

PRIV.20 Uses and disclosures consistent with notice [§ 164.502\(i\)](#)

HIPAA Requirement

Standard: uses and disclosures consistent with notice. A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by [§ 164.520\(b\)\(1\)\(iii\)](#) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

AMC Explanation of HIPAA Regulation

Each covered entity is required to post and distribute a statement of privacy practices describing the covered entity's duties and individuals' rights regarding the use and disclosure of protected health information. All uses and disclosures of protected health information must be consistent with this statement.

§ 164.520 describes the requirements for notices of privacy practices, and § 164.520(b)(1)(iii)(A)-(C) describe the requirements for specific notices of intended use or disclosure of protected health information for: (A) reminders to individuals regarding appointments, and information about treatment alternatives or other health-related benefits; (B) fund-raising; or (C) reports by a group health plan, health insurance issuer, or HMO to the sponsor of the plan.

Key Issues

- ◆ What will be needed to ensure that privacy practices are consistent with required published statements of privacy practices?

Category I Guidelines-Actions must be taken to address these

- ◆ Ensure that the covered entity's privacy practices with respect to use and disclosure of protected health information are consistent with its notices of privacy practices.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider developing and implementing measures to determine how well practice conforms to the notice (e.g. surveys, counts of complaints of deviation).

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

PRIV.21 Disclosures by whistleblowers and workforce member crime victims **§ 164.502(i)**

HIPAA Requirement

Standard: disclosures by whistleblowers and workforce member crime victims.

(1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

AMC Explanation of HIPAA Regulation

This section shields the covered entity from action for disclosures made by whistleblowers as part of the reporting of a violation. If a workforce member of an AMC discloses protected health information to a health oversight agency or to an attorney in the process of reporting either an allegation of unlawful conduct by the covered entity, or a violation of professional standards or clinical standards, or conditions in the covered entity that endanger patients, then the disclosure is not treated as a violation of the regulations by the covered entity.

In addition, a workforce member who is a victim of a crime may disclose identifying protected health information about the suspected perpetrator to a law enforcement official, and such disclosure is not considered to be a violation of the regulations. The limitations on the specific information that may be disclosed under the protection of this provision are found in § 164.512(f)(2)(i).

AMC/HIPAA Workgroup

Key Issues

- ◆ What civil liability could covered entities have for harm from the breach, even if they are shielded under the regulations?

Category I Guidelines-Actions must be taken to address these

- ◆ Covered entities are not required to do anything to comply with this portion of the regulation other than to be aware that such conditions exist and are defined in the regulation.

Category II Guidelines-Actions should be taken to address these

- ◆ Create or bolster internal reporting and compliance programs so as to reduce the need for whistleblower disclosures.
- ◆ Ensure that it is practical for workforce members who are crime victims to limit their disclosures to law enforcement to the items listed in the regulation.
- ◆ When making disclosures under this section, note that the disclosure is made pursuant to this section.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

PRIV.22 Use and disclosure for facility directories [§ 164.510\(a\)](#)

HIPAA Requirement

Standard: use and disclosure for facility directories.

(1) *Permitted uses and disclosure. Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:*

(i) *Use the following protected health information to maintain a directory of individuals in its facility:*

(A) *The individual's name;*

(B) *The individual's location in the covered health care provider's facility;*

(C) *The individual's condition described in general terms that does not communicate specific medical information about the individual; and*

(D) *The individual's religious affiliation; and*

(ii) *Disclose for directory purposes such information:*

(A) *To members of the clergy; or*

(B) *Except for religious affiliation, to other persons who ask for the individual by name.*

(2) *Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.*

(3) *Emergency circumstances.*

(i) *If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:*

(A) *Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and*

(B) *In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.*

(ii) *The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.*

AMC Explanation of HIPAA Regulation

A covered entity (typically a hospital) may, with limitations, use and disclose selected protected health information to create patient directories for use by clergy and others who ask for patients by name. The covered entity must inform individuals that protected health information may be included in patient directories, and tell them who may see the directory entries, and must allow individuals to restrict or prohibit some or all of the permitted uses or disclosures. In emergency

AMC/HIPAA Workgroup

treatment circumstances or if the patient is incapacitated and thus cannot be notified, the covered entity may use or disclose some or all of the individual's patient directory information with limitations. In such circumstances, the individual must be informed as soon as it is practicable.

Key Issues

- ◆ What mechanisms are needed to ensure that patients can restrict or prohibit use or disclosure of directory information where desired?
- ◆ What criteria will be used to determine that "(t)he individual's condition (is) described in general terms that does (sic) not communicate specific medical information....?"
- ◆ How can printed reports from patient directories be limited to those with a need to see them?

Category I Guidelines-Actions must be taken to address these

- ◆ Limit protected health information in patient directories to name, location in facility, general statement of condition, and religious affiliation.
- ◆ Limit disclosure of religious affiliation to members of the clergy only.
- ◆ Limit other disclosures of protected health information in patient directories to persons who ask for individuals by name.
- ◆ Provide individuals with an opportunity to restrict or prohibit the use of some or all of their protected health information in patient directories unless they are unable to communicate their preferences due to emergency circumstances or incapacity.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish policies and procedures for authenticating members of the clergy.
- ◆ Establish mechanisms that ensure patients' conditions are appropriately described.
- ◆ Consider the meaning of the term "impracticable" as used here. It is generally taken to be a stronger standard than "impractical."
- ◆ Consider routing some inquiries to personnel who have been specially trained to handle sensitive cases.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

PRIV.23 Uses and disclosures for involvement in the individual's care and notification purposes [§ 164.510\(b\)](#)

HIPAA Requirement

Standard: uses and disclosures for involvement in the individual's care and notification purposes.

(1) *Permitted uses and disclosures. (i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.*

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.

(2) *Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:*

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present. If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.*

(4) *Use and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this*

AMC/HIPAA Workgroup

section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

AMC Explanation of HIPAA Regulation

A covered entity may, with limitations, use or disclose (typically to relatives) protected health information for the purposes of notification and involvement in an individual's care. A covered entity may also use professional judgment and its experience with common practice in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information. Finally, a covered entity may, with limitations, use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts.

Key Issues

- ◆ What procedures are needed to ensure that persons do not inappropriately receive protected health information about an individual under the provisions of this section?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop and implement policies and procedures that help ensure appropriate and correct use and disclosure under this section.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop and implement policies and procedures that help ensure that disclosures under this section are not made to inappropriate persons.

Roadblocks

No roadblocks specific to this point.

Comments

Review PRIV.18 for related considerations.

AMC/HIPAA Workgroup

PRIV.24 Uses and disclosures of protected health information for marketing [§ 164.514\(e\)\(1\)](#)

HIPAA Requirement

Standard: uses and disclosures of protected health information for marketing. A covered entity may not use or disclose protected health information for marketing without an authorization that meets the applicable requirements of [§ 164.508](#), except as provided for by paragraph (e)(2) of this section.

(2) Implementation specifications: requirements relating to marketing.

(i) A covered entity is not required to obtain an authorization under § 164.508 when it uses or discloses protected health information to make a marketing communication to an individual that:

(A) Occurs in a face-to-face encounter with the individual;

(B) Concerns products or services of nominal value; or

(C) Concerns the health-related products and services of the covered entity or of a third party and the communication meets the applicable conditions in paragraph (e)(3) of this section.

(ii) A covered entity may disclose protected health information for purposes of such communications only to a business associate that assists the covered entity with such communications.

(3) Implementation specifications: requirements for certain marketing communications. For a marketing communication to qualify under paragraph (e)(2)(i) of this section, the following conditions must be met:

(i) The communication must:

(A) Identify the covered entity as the party making the communication;

(B) If the covered entity has received or will receive direct or indirect remuneration for making the communication, prominently state that fact; and

(C) Except when the communication is contained in a newsletter or similar type of general communication device that the covered entity distributes to a broad cross-section of patients, enrollees, or other broad groups of individuals, contain instructions describing how the individual may opt out of receiving future such communications.

(ii) If the covered entity uses or discloses protected health information to target the communication to individuals based on their health status or condition:

(A) The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and

(B) The communication must explain why the individual has been targeted and how the product or service relates to the health of the individual.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications, under paragraph (e)(3)(i)(c) of this section, are not sent such communications.

AMC/HIPAA Workgroup

AMC Explanation of HIPAA Regulation

The regulations explicitly allow the use of protected health information for targeted (by the health history or status of the recipient) marketing by or for the covered entity without an explicit authorization from the individual. If the marketing is done face-to-face, anything can be marketed; items of nominal value can be marketed without restriction. Otherwise, health related products can be marketed to individuals provided the covered entity is identified, any remuneration to the covered entity is prominently disclosed, and an opt-out capability is included (except for broad newsletters). If protected health information is used to target the health-related product, the covered entity must make a determination that it may be of value for the condition and must explain in the communication why the individual is being targeted.

Key Issues

- ◆ To what does the covered entity want to lend its name?
- ◆ How will the covered entity monitor and control the use of its name?
- ◆ Who will determine if the item has value to the patient?

Category I Guidelines-Actions must be taken to address these

- ◆ For health related products:
 - ▶ Identify the covered entity in the marketing communication.
 - ▶ If the covered entity receives direct or indirect remuneration, state that fact prominently in the communication.
 - ▶ Except for newsletters and the like, offer individuals the opportunity to opt out of future such communications.
 - ▶ Maintain a record of the disclosures.

Category II Guidelines-Actions should be taken to address these

- ◆ Have a central method to manage opt-outs.

Roadblocks

No roadblocks specific to this point.

Comments

This section of the regulations was not in the Notice of Proposed Rulemaking and has not had a real opportunity for comment. Some reviewers see it as overly broad, allowing individuals even less privacy than they have now for video rentals. For these reasons, AMCs should watch this area for changes before investing seriously in implementations.

PRIV.25 Uses and disclosures for fundraising [§ 164.514\(f\)\(1\)](#)

HIPAA Requirement

Standard: uses and disclosures for fundraising. A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of [§ 164.508](#):

- (i) Demographic information relating to an individual; and
 - (ii) Dates of health care provided to an individual.
- (2) ***Implementation specifications: fundraising requirements.*** (i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by [§ 164.520\(b\)\(1\)\(iii\)\(B\)](#) is included in the covered entity's notice;
- (ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.
 - (iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

AMC Explanation of HIPAA Regulation

The covered entity may engage in, or contract for, fundraising for its benefit using protected health information. The covered entity must allow an opt-out feature and provide a means of managing the opt-outs. If the covered entity intends to use demographics and dates of health care in fund-raising, it must include a statement that it plans to do so in the privacy notice.

Key Issues

- ◆ How will the limits placed on fundraising without an authorization affect which fundraising efforts will continue?

Category I Guidelines-Actions must be taken to address these if fundraising is pursued:

- ◆ Include an opt-out method.
- ◆ Make reasonable efforts to ensure that opt-outs are honored across the covered entity.
- ◆ Maintain a record of disclosures.
- ◆ Include a statement in privacy notice if patient information will be used to target patients for receipt of fundraising materials.

Category II Guidelines-Actions should be taken to address these

- ◆ Review the notice of privacy policy to determine whether it permits the use of other protected health information for fundraising.

AMC/HIPAA Workgroup

Roadblocks

Covered entities with decentralized fundraising may find it difficult to implement the opt-out provisions. The language of the regulation may exclude mailings targeted using diagnosis without authorization. If so, this will significantly affect many mailings done today.

Comments

The limits on which information may be used in fund-raising without an authorization may foster the use of authorizations to provide clear permission to use additional information (e.g. diagnosis) or cause some forms of fund-raising activities to stop.

AMC/HIPAA Workgroup

PRIV.26 Uses and disclosures for underwriting and related purposes [§ 164.514\(g\)](#)

HIPAA Requirement

Standard: uses and disclosures for underwriting and related purposes. If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.

AMC Explanation of HIPAA Regulation

When a covered entity receives an individual's protected health information as part of an application for health insurance or other health benefits, and the individual does not obtain insurance or benefits from the covered entity, the covered entity may not use or disclose such protected health information for any other purpose except as required by law.

Key Issues

- ◆ What mechanisms are needed for appropriate disposal or destruction of protected health information received as part of an unsuccessful application process for health insurance or other health benefits?
- ◆ What mechanisms are needed to ensure the appropriate handling of such protected health information in the event of the sale, acquisition, liquidation, or bankruptcy of the covered entity originally receiving the protected health information?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop policies and procedures to limit the use or disclosure of protected health information received as part of an unsuccessful application process for health insurance or other health benefits to only that required by law.

Category II Guidelines-Actions should be taken to address these

None.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

Sub-Section B: Balancing Privacy and Public Responsibility

AMC/HIPAA Workgroup

PRIV.27 Uses and disclosures required by law [§ 164.512\(a\)](#)

HIPAA Requirement

Standard: uses and disclosures required by law.

- (1) *A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.*
- (2) *A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.*

AMC Explanation of HIPAA Regulation

A covered entity may use or disclose protected health information without patient authorization or consent where the use or disclosure is required by law. The use or disclosure must be limited to that required by law and must meet the requirements of one of the following sections:

- § 164.512(c) Disclosures about victims of abuse, neglect, or domestic violence;
- § 164.512(e) Disclosures for judicial or administrative proceedings;
- § 164.512(f) Disclosures for law enforcement purposes.

Key Issues

- ◆ What mechanisms are needed to ensure that only those uses and disclosures required by law are made without individuals' consents or authorization?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish mechanisms to appropriately limit uses and disclosures required by law.
- ◆ Determine the legal relation of the requirements under this section to stricter state laws.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Consider checklists in addition to narrative descriptions of reporting requirements to assist staff in avoiding errors in reporting.
- ◆ Involve legal staff and other knowledgeable individuals to ensure appropriate reporting.
- ◆ Maintain records of all disclosures under this section and the statutory rationale for each.

Roadblocks

No roadblocks specific to this point.

Comments

None.

HIPAA Requirement

Standard: uses and disclosures for public health activities.

(1) Permitted disclosures. *A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:*

(i) *A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;*

(ii) *A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;*

(iii) *A person subject to the jurisdiction of the Food and Drug Administration:*

(A) *To report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations if the disclosure is made to the person required or directed to report such information to the Food and Drug Administration;*

(B) *To track products if the disclosure is made to a person required or directed by the Food and Drug Administration to track the product;*

(C) *To enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals, or other problems); or*

(D) *To conduct post marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration;*

(iv) *A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or*

(v) *An employer, about an individual who is a member of the workforce of the employer, if:*

(A) *The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides a health care to the individual at the request of the employer:*

(1) *To conduct an evaluation relating to medical surveillance of the workplace; or*

(2) *To evaluate whether the individual has a work-related illness or injury;*

(B) *The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;*

AMC/HIPAA Workgroup

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance;

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(1) By giving a copy of the notice to the individual at the time the health care is provided; or

(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(2) Permitted uses. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

AMC Explanation of HIPAA Regulation

In specified situations, a covered entity may disclose (and sometimes use) protected health information for public health activities without an individual's consent or authorization. The permitted *disclosures* are enumerated in the regulation. Permitted *uses* for public health activities exist only where the disclosing covered entity is itself a public health authority, in which case the covered entity is permitted to use all information that it is permitted to disclose under paragraph (b)(1) of this section.

Key Issues

- ◆ How will authorized agencies and individuals and permitted disclosures be identified?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop and implement policies and procedures to ensure that the above reporting requirements are met.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Consider checklists in addition to narrative descriptions of reporting requirements to assist staff in avoiding errors in reporting.
- ◆ Involve legal staff and other knowledgeable individuals to ensure appropriate reporting.
- ◆ Maintain records of all disclosures under this section and the regulatory rationale for each.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

PRIV.29 Disclosures about victims of abuse, neglect, or domestic violence [§ 164.512\(c\)](#)

HIPAA Requirement

Standard: disclosures about victims of abuse, neglect or domestic violence.

(1) Permitted disclosures. Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) Informing the individual. A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

AMC Explanation of HIPAA Regulation

Disclosure of protected health information about victims of abuse, neglect, or domestic violence without the individual's consent or authorization is permitted by a covered entity in specified situations. These are described in the regulation. They are also described under § 164.512(c), which addresses reporting to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect. In instances where the covered entity makes disclosures according to the above rules, the covered entity must promptly inform the individual that the disclosure has been made, unless certain enumerated conditions exist.

AMC/HIPAA Workgroup

Key Issues

- ◆ How can complex reporting requirements be efficiently communicated to and executed by staffs with variety of different responsibilities and duties?
- ◆ Who will determine that a reportable event has occurred?
- ◆ Who will make the report?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop and implement detailed policies, procedures, and mechanisms for permitted reporting.
- ◆ Develop a process for informing the individual about public health reports, making the report, and deciding whether or not to inform the individual.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Consider flow charts in addition to narrative descriptions of reporting requirements to assist staff in avoiding errors in reporting.
- ◆ Involve legal staff and other knowledgeable individuals to ensure appropriate reporting.
- ◆ Document the fact that the report was made or that a decision was made not to report.
- ◆ Determine for your organization who will determine that a reportable event has occurred.

Roadblocks

No roadblocks specific to this point.

Comments

None.

HIPAA Requirement

Standard: uses and disclosures for health oversight activities.

(1) Permitted disclosures. *A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:*

(i) *The health care system;*

(ii) *Government benefit programs for which health information is relevant to beneficiary eligibility;*

(iii) *Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or*

(iv) *Entities subject to civil rights laws for which health information is necessary for determining compliance.*

(2) Exception to health oversight activities. *For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:*

(i) *The receipt of health care;*

(ii) *A claim for public benefits related to health; or*

(iii) *Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.*

(3) Joint activities or investigations. *Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.*

(4) Permitted uses. *If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.*

AMC Explanation of HIPAA Regulation

Entities may disclose protected health information without consent or authorization for certain specified health oversight activities.

Key Issues

- ◆ Who will determine what disclosures are permitted, and what may be disclosed?
- ◆ How will this information be released and who will determine that it is released in a way that minimizes risk?
- ◆ Who are the relevant oversight bodies and what oversight are they exercising?

AMC/HIPAA Workgroup

Category I Guidelines-Actions must be taken to address these:

- ◆ Develop and document a policy and process compliant with the requirements of this section for the disclosure of protected health information for health oversight activities.
- ◆ Maintain a record of disclosures for health oversight activities; section § 164.528 implies the need to be able to provide a record of these disclosures as part of the disclosure history that entities must provide to individuals on request.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Document all disclosures and the rationale for health oversight activities.

Roadblocks

Determining what “health oversight activities” means may be difficult.

Comments

De-identified data could perhaps be used in this area.

PRIV.31 Disclosures for judicial and administrative proceedings [§ 164.512\(e\)](#)

HIPAA Requirement

Standard: disclosures for judicial and administrative proceedings.

(1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(1) No objections were filed; or

(2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

AMC/HIPAA Workgroup

(v) *For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:*

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) Other uses and disclosures under this section. The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

AMC Explanation of HIPAA Regulation

Entities may disclose protected health information for specific judicial and administrative proceedings, though with restrictions. The requesting party must “assure” the covered entity that there have been reasonable attempts to contact the subject of the records and allow him or her an opportunity to formally object to the disclosure. A covered entity may seek to notify the patient to provide this opportunity. The request must be refused unless the requestor agrees to limit uses and disclosures to the needs of the proceeding and to destroy or return protected health information at the end of the proceeding.

Key Issues

- ◆ Who will determine what is permitted for disclosure under this point?
- ◆ How will this protected health information be released, and who will determine that it is released in a way that minimizes risk?
- ◆ Who will determine whether the requestor has made “satisfactory assurance?”
- ◆ How will a covered entity ensure that the protected health information is returned or destroyed?
- ◆ What duty to mitigate harm does a covered entity have with regard to potential inappropriate further disclosures by the requesting party?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop and document a policy and process compliant with the requirements of this section for the disclosure of protected health information for judicial and administrative proceedings.

AMC/HIPAA Workgroup

- ◆ Maintain a record of disclosures for judicial and administrative proceedings; § 164.528 implies the need to have a record of these disclosures as part of the disclosure history that entities must provide to individuals on request.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Document all disclosures for judicial and administrative proceedings.
- ◆ Request either return of the disclosed protected health information or assurance that the protected health information has been destroyed.

Roadblocks

Ensuring consistent practice across the AMC, determining that “satisfactory assurances” have taken place, and coordinating such disclosures across the AMC may prove unwieldy if not properly assessed and organized.

Comments

Some disclosure requests of this type will likely be ones that the patient makes in order to support his or her claims in a proceeding. Other requests may be ones that patients will object to because of the potential that the disclosure will not favor their interests in a proceeding. Because of this tension, AMCs should consider having a sound and readily defensible system for managing these disclosures.

PRIV.32 Disclosures for law enforcement purposes § 164.512(f)

HIPAA Requirement

Standard: disclosures for law enforcement purposes. A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) *Permitted disclosures: pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:

(i) *As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or*

(ii) *In compliance with and as limited by the relevant requirements of:*

(A) *A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;*

(B) *A grand jury subpoena; or*

(C) *An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:*

(1) *The information sought is relevant and material to a legitimate law enforcement inquiry;*

(2) *The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and*

(3) *De-identified information could not reasonably be used.*

(2) *Permitted disclosures: limited information for identification and location*

purposes. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) *The covered entity may disclose only the following information:*

(A) *Name and address;*

(B) *Date and place of birth;*

(C) *Social security number;*

(D) *ABO blood type and rh factor;*

(E) *Type of injury;*

(F) *Date and time of treatment;*

(G) *Date and time of death, if applicable; and*

(H) *A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.*

(ii) *Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's*

AMC/HIPAA Workgroup

DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) *Permitted disclosure: victims of a crime. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:*

(ii) The individual agrees to the disclosure; or

(iii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) *Permitted disclosure: decedents. A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.*

(5) *Permitted disclosure: crime on premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.*

(6) *Permitted disclosure: reporting crime in emergencies.*

(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

AMC Explanation of HIPAA Regulation

AMCs can, and in some cases must, disclose protected health information for law enforcement purposes. This section prescribes the conditions when protected health information can be

AMC/HIPAA Workgroup

disclosed. These disclosure conditions include: when required by law; in compliance with a court order, grand jury subpoena, or administrative request (when certain restrictions and conditions are met); limited information for identification and location purposes; disclosures by victims of a crime; disclosures based on suspicion that decedent's death was caused by a criminal act or that a crime was conducted by the individual, and reporting a crime in an emergency. Covered entities may not disclose DNA information, dental records, or tissue or body fluid samples under this provision.

Key Issues

- ◆ Who will determine what can and must be disclosed?
- ◆ Who will determine that the information sought is “relevant,” “specific,” “limited,” and that the purpose requires protected health information instead of de-identified information?
- ◆ How will the covered entity determine that the disclosure of a victim's protected health information is in the victim's best interest?
- ◆ How will release of this protected health information be controlled and documented?
- ◆ How will the covered entity be assured that the released protected health information is protected and then destroyed in a compliant manner?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop policies and processes compliant with the requirements of this section for releasing protected health information to law enforcement agencies.
- ◆ Maintain a record of disclosures for law enforcement purposes; § 164.528 implies the need to have a record of these disclosures as part of the disclosure history that entities must provide to individuals on request.
- ◆ Determine if de-identified information would be adequate prior to making any disclosure.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Request law enforcement agencies to return disclosed protected health information or report that the protected health information has been destroyed.
- ◆ Require law enforcement agencies to sign an agreement that they will follow standards to safeguard the disclosed protected health information.

Roadblocks

Failing to ensure consistent interpretation of the terms “relevant,” “specific,” and “limited,” across the AMC will create confusion, and coordinating disclosures across the AMC will require open communication and collaboration.. Determining when the request requires protected health information instead of de-identified information can be difficult.

Comments

Disclosures of this type are likely to have significant results for the parties involved. AMCs should have procedures to ensure that their practices comply with the regulations with a high

AMC/HIPAA Workgroup

degree of accuracy. The alternative may be knowing improper disclosure of protected health information by the covered entity—which is a felony under HIPAA.

AMC/HIPAA Workgroup

PRIV.33 Uses and disclosures about decedents [§ 164.512\(g\)](#)

HIPAA Requirement

Standard: uses and disclosures about decedents.

(1) Coroners and medical examiners. *A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.*

(2) Funeral directors. *A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.*

AMC Explanation of HIPAA Regulation

Protected health information about a deceased person can only be used or disclosed as described here or for other uses and disclosures required by law (§ 164.512(a)). Except for the specific disclosures here, these regulations apply the same standard to protected health information about a deceased person as they do to protected health information pertaining to a living person.

Key Issues

- ◆ How will the entity authenticate coroners and medical examiners?
- ◆ How will the entity authenticate funeral directors?
- ◆ What protected health information about the deceased individual do the coroners, medical examiners, and funeral directors need?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop policies and procedures for determining what information should be released to whom it should be released, as well as how such releases should be documented.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Develop a list of the minimum necessary protected health information to disclose to funeral directors.

Roadblocks

No roadblocks specific to this point.

AMC/HIPAA Workgroup

Comments

Uses and disclosures specifically allowing for research are covered in PRIV.35. An executor or estate administrator must be treated as a personal representative per § 164.502(g)(4).

Prior to this regulation, the privacy rights of an individual under federal law ended with death; their data were available under the Freedom of Information Act. States may have more restrictive provisions.

AMC/HIPAA Workgroup

PRIV.34 Uses and disclosures for cadaveric organ, eye, or tissue donation purposes **[§ 164.512\(h\)](#)**

HIPAA Requirement

Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes. A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

AMC Explanation of HIPAA Regulation

AMCs can release protected health information to organ procurement agencies to facilitate cadaveric tissue donation. Such information is essential to the determination of usefulness of harvested organs, eyes, or tissue.

Key Issues

- ◆ How and where will such disclosures be documented?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop policies and procedures on how protected health information will be disclosed for the purpose of cadaveric tissue donation.

Category II Guidelines-Actions should be taken to address these

- ◆ Determine if minimum necessary disclosure is appropriate for procurement, banking, and transport resources purposes since the scope of their involvement may be limited.
- ◆ The actual transport team should be considered as the treatment team for whom the complete disclosure of protected health information is appropriate.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

PRIV.35 Uses and disclosures for research purposes [§ 164.512\(i\)](#)

HIPAA Requirement

Standard: uses and disclosures for research purposes.

(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) Research on decedent's information. The covered entity obtains from the researcher:

(A) Representation that the use or disclosure is sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under

AMC/HIPAA Workgroup

paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) Identification and date of action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than minimal risk to the individuals;

(B) The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;

(C) The research could not practicably be conducted without the alteration or waiver;

(D) The research could not practicably be conducted without access to and use of the protected health information;

(E) The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;

(F) There is an adequate plan to protect the identifiers from improper use and disclosure;

(G) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

(H) There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.

(iii) Protected health information needed. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(D) of this section;

(iv) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR

AMC/HIPAA Workgroup

219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) Required signature. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

AMC Explanation of HIPAA Regulation

This section describes the process for the use or disclosure of protected health information in research without specific authorization from the individual. The first four waiver criteria listed above [164.512(I)(2)(ii)(A-D)] for approval of use of protected health information without authorization already appear in the Common Rule. Waiver criterion (E) is already required of all protocols reviewed by the IRB or privacy board. The last three represent additional criteria not explicitly addressed in the Common Rule, but often found in research protocols. Existing IRBs or new privacy boards will need to review research protocols for compliance with privacy requirements. “Reviews preparatory to research” and “research on decedent’s information” require notification of the covered entity for use or disclosure. Receiving and monitoring these notifications may fall to the IRB or Privacy Board. Entities having any federally funded projects involving human subjects are required to have an IRB. If an entity does not already have an IRB, then it will be required to have a privacy board.

Key Issues

- ◆ How should the intersection of research (IRB-based) privacy protocols and clinical privacy protocols be managed?
- ◆ How is the IRB or privacy board going to handle the increased workload?
- ◆ How can § 164.512(ii)(B) be accomplished in this electronic age?

Category I Guidelines-Actions must be taken to address these

- ◆ Ensure that the IRB or Privacy Board reviews relevant research proposals before researchers can obtain any protected health information.
- ◆ Provide training and funding to the IRB or Privacy Board so it can perform these duties.

AMC/HIPAA Workgroup

Category II Guidelines – Areas where policies should be considered

- ◆ Update the IRB processes and documentation to reflect these new requirements.
- ◆ For research planning, consider using de-identified protected health information at the earliest opportunity in the data gathering cycle.

Roadblocks

Additional costs related to compliance will be viewed as having a negative effect on the research enterprise.

Comments

The “reviews preparatory to research” can be used to generate pilot data for research projects or to address “case finding” in clinical trials. The notice must be obtained by the covered entity; the recipient of this notice is likely to be the IRB. Similarly, “research on decedent’s information” requires notification of the covered entity.

Although the headings of the various sections use the term “waiver,” the text states “alteration to or waiver.” This allows the IRB or Privacy Board to modify the requirements related to authorizations for research in sections of § 164.508 to approve, for instance, research using verbal informed consent [a modification to § 164.508(c)(1)(vii)].

AMC/HIPAA Workgroup

PRIV.36 Uses and disclosures to avert a serious threat to health or safety [§ 164.512\(j\)](#)

HIPAA Requirement

Standard: uses and disclosures to avert a serious threat to health or safety.

(1) Permitted disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)

(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) Use or disclosure not permitted. A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) Limit on information that may be disclosed. A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) Presumption of good faith belief. A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

AMC Explanation of HIPAA Regulation

Covered entities can release protected health information to prevent or lessen a serious and imminent threat to the health or safety of a person or of the public. This section prescribes the conditions under which such disclosures are permitted. There is a presumption in this standard that the entity is acting in good faith.

AMC/HIPAA Workgroup

Key Issues

- ◆ Who will determine if the disclosure is permitted or not?
- ◆ How will permitted releases of protected health information be documented?
- ◆ How will “good faith” be determined and documented?
- ◆ What conditions must exist for counselors and therapists to be permitted to disclose protected health information provided to them in the course of treatment?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop policies and procedures on how protected health information can be disclosed to avert a serious threat to health and safety.

Category II Guidelines-Actions should be taken to address these

None.

Roadblocks

No roadblocks specific to this point.

Comments

None.

HIPAA Requirement

Standard: uses and disclosures for specialized government functions.

Military and veterans activities.

(i) Armed Forces personnel. *A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information:*

(A) *Appropriate military command authorities; and*

(B) *The purposes for which the protected health information may be used or disclosed.*

(ii) Separation or discharge from military service. *A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.*

(iii) Veterans. *A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.*

(iv) Foreign military personnel. *A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the Federal Register pursuant to paragraph (k)(1)(i) of this section.*

(2) National security and intelligence activities. *A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).*

(3) Protective services for the President and others. *A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.*

(4) Medical suitability determinations. *A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was*

AMC/HIPAA Workgroup

determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

- (i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;*
- (ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or*
- (iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.*

Correctional institutions and other law enforcement custodial situations.

(i) Permitted disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

- (A) The provision of health care to such individuals;*
- (B) The health and safety of such individual or other inmates;*
- (C) The health and safety of the officers or employees of or others at the correctional institution;*
- (D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;*
- (E) Law enforcement on the premises of the correctional institution; and*
- (F) The administration and maintenance of the safety, security, and good order of the correctional institution.*

(ii) Permitted uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) No application after release. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

Covered entities that are government programs providing public benefits.

(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or

AMC/HIPAA Workgroup

to improve administration and management relating to the covered functions of such programs.

AMC Explanation of HIPAA Regulation

This section prescribes the circumstances under which protected health information can be used or disclosed for specialized government functions, including military and veterans activities, correctional institutions and other law enforcement custodial situations, and covered entities that are government programs providing public benefits. Additionally, this section addresses release issues for covered entities within the Department of Veterans Affairs.

Key Issues

- ◆ Who will determine if the appropriate military authority has been established?
- ◆ Who will determine whether an individual is an “authorized federal official?”
- ◆ How can correctional facilities ensure that protected health information of released inmates is no longer available for use or disclosure?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop policies and procedures for the use and disclosure of protected health information for specialized government functions.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Ensure that written and approved procedures are in place and available to all personnel associated with these agencies.
- ◆ Collaborate with specialized government agencies for effective transmission, use, and disclosure of protected health information.

Roadblocks

No roadblocks specific to this point.

Comments

The following references provide additional material relevant to this guideline:

- ◆ National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).
- ◆ 18 U.S.C. 3056, 22 U.S.C. 2709(a)(3), 18 U.S.C. 871 and 879.
- ◆ Executive Orders 10450 and 12698.
- ◆ §§ 101(a)(4) and 504 of the Foreign Service Act.
- ◆ §§ 101(b)(5) and 904 of the Foreign Service Act.

AMC/HIPAA Workgroup

PRIV.38 Disclosures for workers' compensation [§ 164.512\(l\)](#)

HIPAA Requirement

Standard: disclosures for workers' compensation. A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

AMC Explanation of HIPAA Regulation

Releases of protected health information that are required by workers' compensation laws are excluded from the general rule against disclosure of protected health information. This standard permits a covered entity to disclose protected health information to satisfy the conditions of work-related compensation as required by law.

Key Issues

- ◆ To whom can a covered entity release workers' compensation-related protected health information?
- ◆ What are the covered entity's responsibilities if protected health information provided to an authorized compensation agency or service is improperly handled or disclosed?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop a process and procedure for disclosure of the minimum necessary protected health information when it is requested by an authorized compensation agency.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish procedures for authenticating requests for disclosure of protected health information that is required or permitted under this section.
- ◆ Confirm the existence of written policies and procedures that delineate responsibility and that identify that consent or authorization are not required when protected health information is disclosed to a lawful compensation agency.
- ◆ Communicate the covered entity's understanding of the standard to associated workers' compensation agencies.

Roadblocks

No roadblocks specific to this point.

Comments

None.

PRIV.39 **Minimum necessary [§ 164.502\(b\)](#)**

HIPAA Requirement

Standard: minimum necessary. (1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

- (i) Disclosures to or requests by a health care provider for treatment;*
- (ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section, as required by paragraph (a)(2)(i) of this section, or pursuant to an authorization under [§ 164.508](#), except for authorizations requested by the covered entity under § 164.508(d), (e), or (f);*
- (iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter (see AMC Explanation below);*
- (iv) Uses or disclosures that are required by law, as described by [§ 164.512\(a\)](#); and*
- (v) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.*

AMC Explanation of HIPAA Regulation

This regulation requires that entities must make reasonable efforts to ensure that the minimum necessary protected health information is disclosed or used for any reason except disclosure to a provider for treatment, disclosure to the patient, disclosures made to HHS pursuant to a privacy investigation, or disclosures required by other law or these regulations. (Note: Use of protected health information for treatment appears to be subject to the minimum necessary provisions). Policies must be created and implemented that define the conditions in which necessary disclosures will be permitted to achieve a specified purpose. § 164.514(d), covered later in this document, provides implementation specifications for use, disclosure, and requests.

Key Issues

- ◆ How will entities know what quantity of protected health information is reasonable for current needs or reasonably projected future needs?
- ◆ What measures must a covered entity take to ensure that reasonable protections are applied?
- ◆ How adaptive must policies be to be sufficiently flexible for thoughtful interpretation among covered entities?
- ◆ What documentation of process and decisions is needed?

Category I Guidelines-Actions must be taken to address these

- ◆ Create and implement policies that identify and manage uses and disclosure of protected health information to which the minimum necessary standard does and does not apply.

AMC/HIPAA Workgroup

Category II Guidelines-Actions should be taken to address these

- ◆ Routinely monitor procedures and practices related to managing the minimum necessary standard for effectiveness.
- ◆ Use technology, where appropriate, to restrict the flow of protected health information and to manage an accounting of what protected health information is shared with covered entities.
- ◆ Ensure that the right balance is struck between making protected health information needed for care available and ensuring that inappropriate access is inhibited.

Roadblocks

Ensuring that the right balance is struck between providing needed access and inhibiting inappropriate access will be difficult, especially for protected health information that is needed infrequently but is essential and urgent when needed.

Comments

This point in the regulations has created a good deal of concern among provider organizations. It is worth comparing this point to the typical “need to know” policy in a typical provider organization today. The typical “need to know” policy limits the allowed access to information to the amount that a workforce member needs to do their job. Electronic information systems may help enforce this policy by not allowing access at all to protected health information that a specific user does not have a categorical need for (e.g., admitting clerks do not need to know discharge diagnosis). In addition to the technical restriction, workforce members are obligated by policies on conduct to limit their actual access to that which is needed for their jobs. In some systems today, audit logs are used to detect patterns of inappropriate access.

The standard outlined in this point is very similar to the “need to know” policy. The key difference for provider organizations is that failure to enforce the policy is now a regulatory matter. For end users, the key difference is that using one’s technical access capability to inappropriately access and/or disclose protected health information is now a felony instead of simply being a violation of employer policies.

PRIV.40 De-identification of protected health information § 164.514 (a)

HIPAA Requirement

(a) Standard: de-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)

(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

AMC/HIPAA Workgroup

- (M) Device identifiers and serial numbers;*
- (N) Web Universal Resource Locators (URLs);*
- (O) Internet Protocol (IP) address numbers;*
- (P) Biometric identifiers, including finger and voice prints;*
- (Q) Full face photographic images and any comparable images; and*
- (R) Any other unique identifying number, characteristic, or code; and*
- (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.*
- (c) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:*
 - (1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and*
 - (2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.*

AMC Explanation of HIPAA Regulation

Information that is de-identified as defined in the regulation is no longer considered to be protected health information, and is thus exempt from the other provisions of the regulation. The regulation describes two methods of de-identifying information.

Key Issues

- ◆ In what situations will de-identification be used?
- ◆ Who will perform the de-identification? Using what methods and techniques?
- ◆ De-identified information used for human subject research still requires IRB oversight; how will review under HIPAA be carried out?
- ◆ How will Common Rule differences be handled?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop and implement policies, procedures, organizational structures, and processes for determining when and how to de-identify protected health information.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop methods for monitoring the efficacy of de-identification strategies and for remedying failures to adequately de-identify.
- ◆ Be aware of and make use of “more advanced statistical techniques.”
- ◆ Consider how to qualify people to do disclosure analysis.

Roadblocks

No roadblocks specific to this point.

AMC/HIPAA Workgroup

Comments

“Individually identifiable” is defined in HIPAA as follows: “...identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.”

“De-identified” as defined in these regulations (including the “re-identification” code) is considered to be “coded” by IRBs in current interpretation (see reference [3]), and is subject to IRB review.

Extensive relevant experience and expertise exists under the rubric of “disclosure analysis,” which deals with techniques for avoiding disclosure of confidential information about individuals and corporate entities with the release of statistical tabulations and data extractions. The references provided in the regulations are key to any use of disclosure analysis; see FR 65, page 82709 (and below).

The ability to create de-identified data is provided to the covered entity under the operations activities of the consent for healthcare, billing, and operations.

Some states may have de-identification criteria that are more stringent than the safe harbor method. Be aware of those differences if the de-identified data are to be used in another state.

The regulations depend upon the following definitions, which differ from those used in the Common Rule:

- a) Anonymous data: Health information that has never been labeled with patient/subject identifiers.
- b) Anonymized data: Health information where the identifiers have been removed and no means exists for re-identifying patients/subjects.
- c) De-identified data: Health information where the identifiers have been removed but means exist for re-identifying patients/subjects if required. (The National Bioethics Advisory Commission describes this as “coded data.” in its guidelines for IRBs on genetic research. OHRP has adopted that guideline for all research under its auspices [see Reference 3].)

Re-identification of de-identified data would be permitted under appropriate circumstances; for example, patient care where misdiagnosis is discovered in the course of a research study.

References

(1) *Statistical Policy Working Paper 22 - Report on Statistical Disclosure limitation Methodology* (<http://www.fcs.gov/working-papers/wp22.html>) (prepared by the Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology, Office of Management and Budget).

(2) *Checklist on Disclosure Potential of Proposed Data Releases* (http://www.fcs.gov/docs/checklist_799.doc) (prepared by the Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology, Office of Management and Budget).

AMC/HIPAA Workgroup

(3) *Research Involving Human Biological Materials: Ethical Issues and Policy Guidance*, August 1999 (available at <http://bioethics.gov/pubs.html>).

PRIV.41 Minimum necessary requirements [§ 164.514\(d\)\(1\)](#)

HIPAA Requirement

Standard: minimum necessary requirements. A covered entity must reasonably ensure that the standards, requirements, and implementation specifications of § 164.502(b) and this section relating to a request for or the use and disclosure of the minimum necessary protected health information are met.

Implementation specifications: minimum necessary uses of protected health information.

(i) A covered entity must identify:

- (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and
- (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) Implementation specification: minimum necessary disclosures of protected health information. (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

- (A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and
- (B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

- (A) Making disclosures to public officials that are permitted under [§ 164.512](#), if the public official represents that the information requested is the minimum necessary for the stated purpose(s);
- (B) The information is requested by another covered entity;
- (C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or
- (D) Documentation or representations that comply with the applicable requirements of [§ 164.512\(i\)](#) have been provided by a person requesting the information for research purposes.

AMC/HIPAA Workgroup

(4) *Implementation specifications: minimum necessary requests for protected health information.*

(i) *A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.*

(ii) *For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.*

(iii) *For all other requests, a covered entity must review the request on an individual basis to determine that the protected health information sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.*

(5) *Implementation specification: other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.*

AMC Explanation of HIPAA Regulation

This point in the regulations covers the implementation specifications for using, disclosing, and requesting protected health information. The general requirement on minimum use/disclosure is in § 164.502(b). The covered entity must categorize users by their “need to know” profile and establish policies that reasonably limit inappropriate access to protected health information based on the listed categories. Covered entities must also limit their own requests for disclosure from other entities to the minimum needed. Finally, no use, disclosure, or request for a complete medical record is considered minimal unless it is specifically justified as minimal.

Key Issues

- ◆ Are policies, procedures, and practices with respect to “minimum necessary” use or disclosure consistent with appropriate care for all patients and categories of patients?
- ◆ Do policies, procedures, and practices unnecessarily deter, inhibit, or restrict research use of protected health information?
- ◆ Are criteria for minimum disclosure defined, or left to judgment? If they are left to judgment, how is judgment exercised?
- ◆ What monitoring mechanisms can be used to assure appropriate application of the minimum necessary disclosure principle?

Category I Guidelines-Actions must be taken to address these

- ◆ Identify appropriate persons to determine what protected health information should be used, disclosed, and requested consistent with the minimum necessary standard.
- ◆ Ensure that the persons identified under paragraph (b)(2)(i) of this section make the minimum necessary determinations, when required.

AMC/HIPAA Workgroup

- ◆ Within the limits of the covered entity’s technological capabilities, provide for the making of such determinations individually.
- ◆ Define and implement only reasonable policies; the regulations don’t require entities to accept unreasonable cost or disruption in pursuit of this objective.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop and implement policies and procedures for uses and disclosures that are covered in the various other subsections on uses and disclosures. Key articles are:
 - ▶ § 164.508(a)(1) deals with authorizations for use or disclosure initiated by the affected individual.
 - ▶ § 164.514 deals with access of individuals to their own protected health information, but only mentions copying costs for records.
 - ▶ § 164.522 is a section entitled “Rights to request privacy protection for protected health information.”
 - ▶ § 164.510 describes uses and disclosures permitted without individual authorization. Subsections are devoted to: public health; health oversight; judicial proceedings; coroners and medical examiners; law enforcement; government health data systems; directories; payment; research; emergencies; next-of-kin; other disclosures required by law; application to specialized classes (DOD, VA, other government workers).

Roadblocks

For many patient care situations and human-subjects research questions, the “minimum necessary” data becomes apparent only in retrospect. This implies that one may have to initially provide access to more data than is permissible to use in every case. The accessor must be constrained by policy from accessing information in each case that is beyond the minimum needed for his or her task. Also, there appear to be conflicting societal expectations regarding malpractice or negligence where additional data use may prevent patient injury.

Comments

The implementation specifications on minimum disclosure given in this section make the procedural and policy requirements pretty clear. Burdensome and onerous implementations are not required; use the reasonableness principle to guide the development of technique in meeting this requirement.

PRIV.42 Verification requirements [§ 164.514\(h\)\(1\)](#)

HIPAA Requirement

Standard: verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) Implementation specifications: verification.

(i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in [§ 164.512\(f\)\(1\)\(ii\)\(C\)](#) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by [§ 164.512\(i\)\(2\)](#) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

AMC/HIPAA Workgroup

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with [§ 164.510](#) or acts on a good faith belief in making a disclosure in accordance with [§ 164.512\(j\)](#).

AMC Explanation of HIPAA Regulation

This standard requires reasonable assurances, whether in writing or by official document, of the identity and authority of any party requesting protected health information. It also explains the circumstances under which a public official may request information.

Key Issues

- ◆ What reasonable measures will be used to verify the identity of a requesting individual or entity if the requestor is not commonly known to the covered entity?
- ◆ What means will be used to evaluate professional judgment in the absence of the required documentation or identification of an entity requesting protected health information?
- ◆ Under what circumstances can a covered entity be reassured that public officials are authorized to request protected health information verbally and without a written statement?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop policies and procedures for verifying identity and authority of requestors:
 - ▶ Obtain representation or documentation of purpose from any person requesting protected health information under this regulation;
 - ▶ Verify the identity of persons requesting protected health information before giving them access;
 - ▶ Confirm that persons acting on behalf of a public official have appropriate statements on official letterhead before providing them with protected health information;
 - ▶ Establish a policy that legal authority is presumed when a request is made relative to a legal proceeding, warrant, subpoena, or order;
 - ▶ Develop a formal process to authorize disclosure in the absence of a written verification;
 - ▶ Make good faith efforts to identify the people requesting disclosure and the circumstances of disclosure as provided in this section.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop policies that clearly define what sources of identification and what documents of authority can be used to verify permission for disclosure.
- ◆ Provide comprehensive guidelines and back-up resources to assist with questions of verification.

AMC/HIPAA Workgroup

- ◆ When protected health information is released to a legal authority without valid consent, send a cover letter with the material containing a reminder to the recipients that the information is of a sensitive nature and must be handled as such. Retain a copy of the letter for the record.
- ◆ Consider existing processes for disclosure under this section in concert with verifications for parties to whom protected health information is disclosed.
- ◆ Brief frequent requestors of information on the procedural changes required under this standard.

Roadblocks

No roadblocks specific to this point.

Comments

There is a need to provide resources and support for front line workforce implementing these guidelines.

AMC/HIPAA Workgroup

Section Four: Consumer Controls

HIPAA Requirement

Standard: notice of privacy practices.

Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) Exception for group health plans.

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in [§ 164.504\(a\)](#) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in [§ 164.504\(a\)](#) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) Exception for inmates. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) Implementation specifications: content of notice.

(1) Required elements. The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) Header. The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

AMC/HIPAA Workgroup

- (ii) Uses and disclosures. *The notice must contain:*
- (A) *A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.*
 - (B) *A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written consent or authorization.*
 - (C) *If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202.*
 - (D) *For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.*
 - (E) *A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by [§ 164.508\(b\)\(5\)](#).*
- (iii) Separate statements for certain uses or disclosures. *If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:*
- (A) *The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;*
 - (B) *The covered entity may contact the individual to raise funds for the covered entity; or*
 - (C) *A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.*
- (iv) Individual rights. *The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:*
- (A) *The right to request restrictions on certain uses and disclosures of protected health information as provided by [§ 164.522\(a\)](#), including a statement that the covered entity is not required to agree to a requested restriction;*
 - (B) *The right to receive confidential communications of protected health information as provided by [§ 164.522\(b\)](#), as applicable;*
 - (C) *The right to inspect and copy protected health information as provided by [§ 164.524](#);*
 - (D) *The right to amend protected health information as provided by [§ 164.526](#);*
 - (E) *The right to receive an accounting of disclosures of protected health information as provided by [§ 164.528](#); and*
 - (F) *The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.*

AMC/HIPAA Workgroup

- (v) Covered entity's duties. *The notice must contain:*
- (A) *A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;*
- (B) *A statement that the covered entity is required to abide by the terms of the notice currently in effect; and*
- (C) *For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with [§ 164.530\(i\)\(2\)\(ii\)](#), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.*
- (vi) Complaints. *The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.*
- (vii) Contact. *The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by [§ 164.530\(a\)\(1\)\(ii\)](#).*
- (viii) Effective date. *The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.*
- (2) Optional elements.
- (i) *In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by [§ 164.512\(j\)\(1\)\(i\)](#).*
- (ii) *For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with [§ 164.530\(i\)\(2\)\(ii\)](#), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.*
- (3) Revisions to the notice. *The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.*
- (c) Implementation specifications: provision of notice. *A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(4) of this section, as applicable.*
- Specific requirements for health plans.

AMC/HIPAA Workgroup

(i) A health plan must provide notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

*Thereafter, at the time of enrollment, to individuals who are new enrollees; and
Within 60 days of a material revision to the notice, to individuals then covered by the plan.*

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(2) Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider;

(ii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iii) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(ii) of this section, if applicable.

(3) Specific requirements for electronic notice. (i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service.

AMC/HIPAA Workgroup

(iv) *The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.*

(d) Implementation specifications: joint notice by separate covered entities. *Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:*

(1) *The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;*

(2) *The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and*

(i) *Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;*

(ii) *Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and*

(iii) *If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.*

(3) *The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.*

(e) Implementation specifications: documentation. *A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity as required by [§ 164.530\(j\)](#).*

AMC Explanation of HIPAA Regulation

Individuals have the right, except as specifically stated, to be notified of the types of uses and disclosures of protected health information that may be made by a covered entity. They also have the right to be notified of their individual rights and the covered entity's legal duties with respect to that information. This section details the specific requirements for wording of this notice as well as statements of individual rights and covered entity obligations. In addition, it addresses the requirements for the provision of this notice (frequency, timing, and documentation).

Key Issues

- ◆ How much of an obligation do covered entities have to be sure that individuals “understand” this notice (e.g. non-English speakers, visually impaired, uncooperative patients)?
- ◆ How can this lengthy notice be incorporated into routine care with a minimum burden to patients, workforce members, and organizations without further complicating an already confusing “front-end” process?

AMC/HIPAA Workgroup

- ◆ How can the process of enabling individuals to exercise the rights required by the regulations be succinctly communicated as part of this notice?
- ◆ What if a covered entity, because of medical urgency, is unable to present this notice on the day of delivery of service as required?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop a policy and procedure to ensure that the required notices are implemented.
- ◆ Notices must have all the elements specifically required by the regulations, and comply with the provision requirements.
- ◆ Covered entities that maintain a customer service or benefits web site must post their notices on the web site and make the notice available electronically.
- ◆ If the entity makes a material change to the notice, the changed notice must be publicized within a specific timeframe specified.

Category II Guidelines-Actions should be taken to address these

- ◆ Include a brief, easy-to-read description of the key elements of the notice with the detailed version, to enhance patients' understanding.
- ◆ Consider incorporating privacy practices into a covered entity's "patient rights" literature and process in order to minimize the expense and inconvenience to both patient and entity and optimize its informational impact.
- ◆ Consider developing a means of accounting for the delivery of this notice as the covered entity delivers it.

Roadblocks

Providers may be reluctant to tell patients their rights for fear of retaliation if those rights are violated. There can also be concern by both providers and patients that "too much" informed consent is a bad thing.

Many AMCs have decentralized websites, and will have to ensure that all sites have privacy notices.

Comments

The only documentation of compliance required by this standard is "...by retaining copies of the notices issued..." More rigorous accounting methods might leave the AMC vulnerable to audit and in fact be unachievable.

The standard text contains significant details regarding implementation requirements.

References: §§ 160.504, 160.202, 164.508, 164.512, 164.522, 164.524, 164.528, and 164.530.

PRIV.44 Confidential communications requirements [§ 164.522\(b\)\(1\)](#)

HIPAA Requirement

Standard: confidential communications requirements.

(i) *A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.*

(ii) *A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual,*

(2) *Implementation specifications: conditions on providing confidential communications.*

(i) *A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.*

(ii) *A covered entity may condition the provision of a reasonable accommodation on:*

(A) *When appropriate, information as to how payment, if any, will be handled; and*

(B) *Specification of an alternative address or other method of contact.*

(iii) *A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.*

(iv) *A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.*

AMC Explanation of HIPAA Regulation

This portion of the regulations requires the covered entity to accept requests for alternative means of communicating with the patient or plan member and to accommodate such requests if they are reasonable. A *health care provider* may not require the patient to reveal the reason for the request, but a *health plan* may require a statement that the plan member believes that disclosure of the protected health information would endanger the patient.

Key Issues

- ◆ How many alternative communications schemes can a covered entity practically accommodate?
- ◆ How well can a covered entity ensure that the agreed upon alternative is used (and not the normal means)?
- ◆ Will some patients avoid care if no reasonable alternative accommodation can be found?

AMC/HIPAA Workgroup

- ◆ What liability will covered entities have if they fail to use the agreed alternative means and a consequent harm befalls the patient?

Category I Guidelines-Actions must be taken to address these

- ◆ Provide a way for patients or plan members to request alternative means of communication, and accommodate such requests if there is a reasonable way to do so.
- ◆ Establish a procedure so all workforce members who are engaging in communications with a patient who has requested and received an agreement to use alternate means of communication are aware of the need to use those channels.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider creating a limited set of alternative communications models and offering these models to patients or plan members requesting alternative means.
- ◆ Consider establishing a referral program for patients whose communications needs the covered entity cannot reasonably accommodate.
- ◆ Create a method of review to determine the effectiveness of alternative means of communication.
- ◆ Consult legal staff about what constitutes a reasonable request.

Roadblocks

Clear definitions of alternative means of communication and their reliable implementation may be challenging.

Comments

This portion of the regulation creates an accommodation for people whose privacy is not assured in their daily lives. Shared voice mail, shared mailboxes, shared faxes, and shared emails are typical in private homes, barracks, and shelters today. Without this accommodation, many of these patients might not seek needed care. The reliability of using the alternative means is a very important issue here since, presumably, the likelihood that harm would result to the patient is high if normal means are used.

Note the distinction between this confidential communications requirement and the "Right of an individual to request restriction of uses and disclosures" in PRIV.11. In the case of communications, covered entities are required to accommodate the request if it is reasonable. In the case of use and disclosure restrictions, the covered entity is not required to agree to the restriction under any circumstances.

HIPAA Requirement

Standard: access to protected health information.

(1) Right of access. *Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:*

(i) *Psychotherapy notes;*

(ii) *Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and*

(iii) *Protected health information maintained by a covered entity that is:*

(A) *Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or*

(B) *Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).*

(2) Unreviewable grounds for denial. *A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.*

(i) *The protected health information is excepted from the right of access by paragraph (a)(1) of this section.*

(ii) *A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.*

(iii) *An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.*

(iv) *An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.*

(v) *An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.*

AMC/HIPAA Workgroup

(3) Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) Review of a denial of access. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) Implementation specifications: requests for access and timely action.

(1) Individual's request for access. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

Timely action by the covered entity.

(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.

(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i)

AMC/HIPAA Workgroup

or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) Implementation specifications: provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Providing the access requested. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) Form of access requested.

(i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

(ii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) Time and manner of access. The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(4) Fees. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;

(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

AMC/HIPAA Workgroup

(iii) *Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.*

(d) Implementation specifications: denial of access. *If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.*

(1) Making other information accessible. *The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.*

(2) Denial. *The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:*

(i) *The basis for the denial;*

(ii) *If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and*

(iii) *A description of how the individual may complain to the covered entity pursuant to the complaint procedures in [§ 164.530\(d\)](#) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in [§ 164.530\(a\)\(1\)\(ii\)](#).*

(3) Other responsibility. *If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.*

(4) Review of denial requested. *If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.*

(e) Implementation specification: documentation. *A covered entity must document the following and retain the documentation as required by [§ 164.530\(j\)](#):*

(1) *The designated record sets that are subject to access by individuals; and*

(2) *The titles of the persons or offices responsible for receiving and processing requests for access by individuals.*

AMC Explanation of HIPAA Regulation

This section provides for the right of an individual to access, inspect, and obtain a copy of the individual's protected health information in the designated record set. There are exceptions to

AMC/HIPAA Workgroup

this requirement, time frames for compliance, and specific required processes that must be put into place as described below.

Key Issues

- ◆ How will this requirement increase workload?
- ◆ What are the liability issues relative to release of protected health information to the patient and how can they be mitigated?
- ◆ What are the financial considerations to comply with this regulation and can those obligations be passed on to the recipient of the protected health information?
- ◆ What requirements will there be to track requests?
- ◆ Will the covered entity be required to notify a requestor of the inclusion of a new record?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop and document policies and processes to receive and act upon an individual's request to access, inspect, and receive a copy of his or her protected health information, including the denial of such requests.
- ◆ Respond to requests within the timeframe specified in the regulation.

Category II Guidelines-Actions should be taken to address these

- ◆ Develop processes to release required protected health information to requestors.
- ◆ Develop legally defensible grounds for denials.
- ◆ Develop processes to review denial of requests.
- ◆ Develop processes to allow for access and appeal of decisions made by the AMC.
- ◆ Identify the authority to release protected health information and process denials and appeals.
- ◆ Consider including a temporary suspension of the patient's right of access to research records in research consent forms.
- ◆ Have the privacy official develop and maintain an inventory of the kinds of data the institution keeps about individuals.

Roadblocks

The liability and cost associated with providing this information may be extensive. The issue may be further complicated by the actual type of record that is maintained (e.g., residents' records, medical students' records, actual attending physicians' records). As an example, AMCs may have information generated by medical students that would be accessible under the rule and that may not be appropriate for release to patients. Physicians may consider the release of total patient information to not be in the best interest of the patient and, in fact, to be counterproductive. Official versus unofficial records need to be identified with consideration given to residents' and medical students' notes and how those records are to be addressed. The AMC will want to have working definitions of reasonableness and timeliness.

Comments

Carefully review the definition of "designated record set" covered in § 164.501. Shadow charts would also be considered designated records sets under this regulation. Things formally

AMC/HIPAA Workgroup

considered informal records might now be considered part of the designated record set under this regulation (student 3x5 cards, PDAs, etc.).

HIPAA Requirement

Standard: right to amend.

(1) Right to amend. *An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.*

(2) Denial of amendment. *A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:*

(i) *Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;*

(ii) *Is not part of the designated record set;*

(iii) *Would not be available for inspection under [§ 164.524](#); or*

(iv) *Is accurate and complete.*

(b) Implementation specifications: requests for amendment and timely action.

(1) Individual's request for amendment. *The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.*

(2) Timely action by the covered entity.

(i) *The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.*

(A) *If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.*

(B) *If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.*

(ii) *If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:*

(A) *The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and*

(B) *The covered entity may have only one such extension of time for action on a request for an amendment.*

(c) Implementation specifications: accepting the amendment. *If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.*

AMC/HIPAA Workgroup

(1) Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) Implementation specifications: denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Denial. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in [§ 164.530\(d\)](#) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in [§164.530\(a\)\(1\)\(ii\)](#).

(2) Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) Recordkeeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the

AMC/HIPAA Workgroup

subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) Future disclosures.

(i) *If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.*

(ii) *If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.*

(iii) *When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.*

(e) Implementation specification: actions on notices of amendment. *A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.*

(f) Implementation specification: documentation. *A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by [§ 164.530\(j\)](#).*

AMC Explanation of HIPAA Regulation

An individual has the right to request amendment of his or her protected health information. Under specified conditions, the entity has the right to deny the request. If none of these conditions apply, then the entity must make the amendment. Specific requirements for addressing these requests, including timely action, accepting the amendment, and informing the individual and others are detailed. In addition, requirements for denying an amendment are outlined.

Key Issues

- ◆ How will workload increase?
- ◆ What guidelines need to be in place to manage an individual's expectations?
- ◆ What will the amendment and correction process involve to track grievances, and to correct and amend records?
- ◆ Who has the right to amend a record?
- ◆ What is the level of effort required to develop and publicize fair information policies?

AMC/HIPAA Workgroup

- ◆ How will covered entities manage the “whistleblower provision?”
- ◆ Will a covered entity permit a person to see who has viewed his or her record (audit trail reports)?
- ◆ How will the amended record be distributed to all those who need to know about the amendment?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop and document policies and processes to receive and act upon an individual’s request to amend their protected health information, including the denial of such requests.
- ◆ Respond to requests within the timeframe specified in the regulation.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider the provision of resources to assist patients with record reviews.
- ◆ Have the privacy official identify processes for retrieving protected health information about individuals pursuant to their request to revise that information.
- ◆ Have the privacy official define a process for evaluating, and accepting or rejecting, requests for correction and implementing corrections.
- ◆ Consider how to deal with the amendment process for paper and electronic records (including requests for removal of a record).
- ◆ Should have a procedure well documented so that it can be executed by workforce members who are unfamiliar with it who do not do it very often.
- ◆ Consider date-stamping requests.

Roadblocks

AMCs may have inadequate document control processes, making obtaining a record in a timely manner difficult.

Comments

It might be worthwhile for a covered entity to look at the ISO document control processes as a source of useful guidance for making and maintaining record control processes (ISO 9001:1994 Sections 4.5.1 and 4.5.2 ISO 9001:2000 Section 4.2.3; www.iso.ch).

PRIV.47 Right to an accounting of disclosures of protected health information
§ 164.528(a)

HIPAA Requirement

Standard: right to an accounting of disclosures of protected health information.

(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in [§ 164.502](#);

(ii) To individuals of protected health information about them as provided in [§ 164.502](#);

(iii) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in [§ 164.510](#);

(iv) For national security or intelligence purposes as provided in [§ 164.512\(k\)\(2\)](#);

(v) To correctional institutions or law enforcement officials as provided in [§ 164.512\(k\)\(5\)](#); or

(vi) That occurred prior to the compliance date for the covered entity.

(2)

(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in [§ 164.512\(d\)](#) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) Implementation specifications: content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for

AMC/HIPAA Workgroup

an accounting, including disclosures to or by business associates of the covered entity.

(2) The accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:

(A) A copy of the individual's written authorization pursuant to [§ 164.508](#); or

(B) A copy of a written request for a disclosure under [§§ 164.502\(a\)\(2\)\(ii\)](#) or [164.512](#), if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, or pursuant to a single authorization under § 164.508, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(c) Implementation specifications: provision of the accounting.

(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) Implementation specification: documentation. A covered entity must document the following and retain the documentation as required by [§ 164.530\(j\)](#):

AMC/HIPAA Workgroup

- (1) *The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;*
- (2) *The written accounting that is provided to the individual under this section; and*
- (3) *The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.*

AMC Explanation of HIPAA Regulation

The regulation establishes a right for an individual to request and receive an accounting of disclosures of his or her protected health information that have occurred either within the last six years, or since compliance was first required for the covered entity, whichever occurred last. Exceptions are allowed for disclosures required to carry out treatment, payment, and health care operations, to the individuals themselves, and for health oversight, national security or intelligence, correctional institutions, and law enforcement as provided elsewhere. The regulation requires that reporting be temporarily suspended if requested by a health oversight agency or law enforcement official. The regulation also permits the covered entity to establish reasonable charges for these reports.

Key Issues

- ◆ How do entities match disclosures against individuals requesting reports? Are current electronic auditing tools satisfactory for computerized records?
- ◆ How do entities validate requests to suspend reporting?
- ◆ How do entities track suspension requests and ensure suspension of requested reports?
- ◆ What does it mean to provide an accounting of disclosures? What information needs to be included in this? Who will be tasked with doing so?
- ◆ How does one explain a complicated audit trail produced by an information system to a patient? Who will do this?
- ◆ Will an organization permit a person to see who viewed his or her record (i.e. provide audit trail reports)?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish policies and procedures to ensure that disclosure records are retained.
- ◆ Maintain a record of all individuals requesting reports of disclosure and the disposition of those requests.
- ◆ On a case-by-case basis, determine whether disclosures must, may, or must not be reported.
- ◆ Establish a process to ensure that all covered disclosures are reported in a timely period.
- ◆ If an extension of the time limit is needed, ensure that the individual is notified of the delay as required by the regulation, and that the extension does not exceed permissible limits.

Category II Guidelines-Actions should be taken to address these

- ◆ Provide a system to audit access control with the ability to report all accesses of a patients record.

AMC/HIPAA Workgroup

- ◆ Publish the covered entity's fair information policy.
- ◆ Establish incident procedures that include reporting and response procedures.
- ◆ Maintain a list of those who access a record.
- ◆ Respond to requests within the timeframe specified in the regulation.
- ◆ Determine if the covered entity will charge for these reports and, if so, establish a basis for all such charges.

Roadblocks

The paper vs. electronic environment presents many issues, particularly to AMCs where both paper and electronic records are often managed in a decentralized way with no common repository that contains all logs of all releases. This will present a problem when patients request a disclosure history and expect it to be produced in a timely manner.

Comments

None.

AMC/HIPAA Workgroup

Section Five: Administrative requirements

PRIV.48 Privacy Official § 164.530(a)(1)(i)

HIPAA Requirement

Standard: Personnel designation

A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity...

...(2) Implementation specification:

A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

AMC Explanation of HIPAA Regulation

The regulation requires the covered entity to appoint an individual to be accountable for the development and implementation of privacy policies and procedures. It also requires that this designation be documented.

Key Issues

- ◆ What are the job responsibilities of the Privacy Official? Is the authority they have been given commensurate with the role?
- ◆ How will the Privacy Official's duties and resources integrate with related functions in the covered entity?
- ◆ What skills and knowledge base does this position require?
- ◆ Will the privacy responsibilities be added to an existing position, or is this a new FTE?
- ◆ What portion of an FTE should be allocated to this position, and how will requirements change over time as the planning phase is supplanted by a long-term operational and maintenance role?
- ◆ What will be the relationship between the Information Security Officer and the Privacy Official?
- ◆ To whom will this position report within the covered entity?
- ◆ Will the Privacy Official also be the contact person for complaints?
- ◆ Will a separate Privacy Official be required for each covered entity's subsidiaries?

Category I Guidelines-Actions must be taken to address these

- ◆ Select a single individual to serve as the privacy official for each covered entity.
- ◆ Designate one privacy official for covered entities that consist of several subsidiaries pursuant to § 164.504(b).
- ◆ Maintain a written or electronic record of privacy official designation(s).

Category II Guidelines-Actions should be taken to address these

- ◆ Create a job description for the privacy official defining the position's role, responsibilities, and reporting relationship(s).
- ◆ The privacy official:
 - ▶ Should work with a committee representing several different components of the covered entity to develop and implement the privacy policy; and

AMC/HIPAA Workgroup

- ▶ Should have a position on the institution's HIPAA Oversight Board.

Roadblocks

In most AMCs, many departments and individuals currently have the ability to draft and implement policies on the use of protected health information. It might be difficult to get all faculty and staff, across all health system entities, to follow the recommendations of the privacy official.

If a covered entity has multiple privacy officials (its subsidiaries are each considered a "covered entity" pursuant to § 164.504(b)), and the entity wishes to standardize privacy matters, it will take a well-coordinated communication effort. From a marketing and customer service standpoint, it may also be important for the covered entity to have a seamless approach to privacy matters.

Comments

Not every covered entity will need to allocate a new position for the Privacy Official. Small providers may wish to delegate these responsibilities to an existing employee, while large entities may create a full-time position. How a covered entity chooses to designate the covered entities under § 164.504(b) is key to deciding how many privacy officials to designate.

AMCs will likely have multiple people with security or privacy responsibilities. Consider how the privacy official's work will be interdependent with those in supporting roles.

The role of Privacy Official will transition from one of program definition and development to one of operational support and maintenance over a period of two to three years. If thoughtfully and faithfully established, the role will fulfill requirements through functional reporting relationships. The Privacy Official's authority and influence are critical; they must be adequate to the task.

AMC/HIPAA Workgroup

PRIV.49 Privacy Contact Person or Office [§ 164.530\(a\)\(1\)\(ii\)](#)

HIPAA Requirement

Standard: Personnel designation...

...A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by [§ 164.520](#).

(2) Implementation specification:

A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

AMC Explanation of HIPAA Regulation

Each covered entity must designate a contact person or office responsible for receiving complaints under the Privacy Standards and who can provide further information about the covered entity's Privacy Notice. The designation must be documented, and a contact name must be listed on the covered entity's Privacy Notice.

Key Issues

- ◆ What are the job responsibilities of the contact person or office? What is the scope of the position's authority within the covered entity?
- ◆ What skills and knowledge base does this position require?
- ◆ Will the privacy responsibilities be added to an existing position, or should a new position be created?
- ◆ What portion of a FTE should be allocated to this position?
- ◆ What will be the relationship between the Information Security Officer, the Privacy Official, and the contact person/office?
- ◆ To whom will this position report to within the covered entity?
- ◆ Will the Privacy Official also be the contact person for complaints? Will information be consistently handled if the Privacy Official and contact person are not the same? Will questions and incidents be consistently documented if the Privacy Official and the contact person are not the same?
- ◆ Is the mechanism for handling complaints a pre-existing mechanism, an adaptation of a current system, or a new process?
- ◆ Will the contact have access to management so that the right individual will hear complaints with foundation?
- ◆ Will a separate privacy contact be required for each of the covered entity's subsidiaries?

Category I Guidelines-Actions must be taken to address these

- ◆ Designate an individual or an office to receive complaints and provide information about matters covered by the covered entity's Notice of Privacy Practices (§ 164.520).
- ◆ Add the contact information to the covered entity's Notice of Privacy Practices.
- ◆ Maintain a written or electronic record of this personnel designation.

AMC/HIPAA Workgroup

Category II Guidelines-Actions should be taken to address these

- ◆ Establish a reporting structure and process to involve persons with appropriate authority to investigate and track complaints.
- ◆ Ensure that the process of responding to complaints is done in a way that is consistent with good public relations practices as well as good privacy policy.
- ◆ Consider adding the reporting responsibility to an existing function or office.

Roadblocks

If a covered entity has multiple privacy contacts (its subsidiaries are each considered a “covered entity” pursuant to § 164.504(b)), and it wishes to standardize privacy matters, doing so will require a well coordinated communication effort. Having a seamless approach to privacy matters may be important for the covered entity from a marketing and customer service standpoint.

Provision of the appropriate level of authority to handle complaints will require a difficult to achieve complex of relations among several units in an AMC (e.g., Risk Management, Compliance Office, Communications, Counsel).

Comments

Not every covered entity will need to allocate a new position for the contact person. Smaller providers may wish to delegate the responsibilities to an existing workforce member while larger entities may create a full-time position. Depending on the size and nature of the covered entity, the Privacy Officer could share this position.

Handling complaints from the public will likely require a specialized process.

References: § 164.512, Content of Notice and § 164.530(e), Sanctions.

PRIV.50 Training on Privacy § 164.530(b)(1)

HIPAA Requirement

Standard: training. A covered entity must train all members of its workforce to carry out their function within the covered entity.

(2) Implementation specifications: training. (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

AMC Explanation of HIPAA Regulation

The regulation requires training of all members of the covered entity's workforce in the covered entity's policies and procedures with respect to protected health information. This includes initial training at the time that the rule becomes applicable, with subsequent training of new workforce members, and retraining as policy and/or procedure changes occur. All members of the workforce must be trained, including employees, volunteers, trainees, and any others. Finally, paragraph (j) requires that documentation of the training be kept in written or electronic form for six years.

Key Issues

- ◆ What are the criteria for judging training efficacy?
- ◆ How can one determine the adequacy of effort by entities?

Category I Guidelines-Actions must be taken to address these

- ◆ Train workforce members on privacy policy and procedure prior to the effective date of the privacy regulations.
- ◆ Thereafter, train new workforce members reasonably soon after they join the covered entity.
- ◆ When significant changes in policy and/or procedure occur, train the affected workforce members as soon as possible after such changes.
- ◆ Document the training in written or electronic form and retain the records for at least six years.

AMC/HIPAA Workgroup

Category II Guidelines-Actions should be taken to address these

- ◆ Consider providing forms of training that help the trainee relate the policy to how they are to behave in their working environment.
- ◆ Consider including training on how to report a privacy problem.
- ◆ Consider “refresher” courses and periodic reminders for workforce members about privacy policy.
- ◆ Consider competency tests to evaluate training effectiveness.

Roadblocks

No roadblocks specific to this point.

Comments

None.

PRIV.51 Safeguards [§ 164.530\(c\)\(1\)](#)

HIPAA Requirement

Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) Implementation specification: safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

AMC Explanation of HIPAA Regulation

A covered entity must establish administrative, technical, and physical safeguards to protect protected health information from unauthorized access or use. These safeguards must be appropriate and reasonable.

A group health plan is excepted from coverage by § 164.530(c) in circumstances where it gets limited amounts of protected health information under conditions described in § 164.530(k).

Key Issues

- ◆ How should a covered entity handle the determination of what is reasonable and appropriate?
- ◆ Is implementing the (proposed) Security regulations an adequate way to address this point in the privacy regulations?

Category I Guidelines-Actions must be taken to address these

- ◆ A covered entity must establish administrative, technical, and physical safeguards to protect the privacy of protected health information from unauthorized use or disclosure. These safeguards must be appropriate and reasonable.

Category II Guidelines-Actions should be taken to address these

- ◆ Engage in a risk analysis (as the proposed Security regulations require) and create and implement a risk management plan for both electronic and non-electronic information assets.
- ◆ Have the privacy official consult on safeguard requirements with the security officer and others responsible for information practices.
- ◆ Ensure that security and privacy officials have the authority necessary to implement effective safeguards.
- ◆ Have the privacy official create a list of reasonably anticipated threats and hazards to privacy of protected health information and unauthorized uses or disclosures.
- ◆ Be aware that many areas of section (g) address specific parts of the safeguards (training, complaints, sanctions, etc.) and consult those sections for details.

AMC/HIPAA Workgroup

Roadblocks

No roadblocks specific to this point.

Comments

This is an overarching requirement making the covered entity responsible for reasonable privacy safeguards. The Security regulations and other aspects of the Privacy regulations provide some of the specifics of what safeguarding entails. Unfortunately, the fact that the final security regulations have not yet been issued makes it less clear to what safeguard standard the entity will be held.

AMC/HIPAA Workgroup

PRIV.52 Complaints to the covered entity [§ 164.530\(d\)\(1\)](#)

HIPAA Requirement

Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

(2) Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

AMC Explanation of HIPAA Regulation

Covered entities must have a process for receiving and documenting complaints concerning their privacy policies and procedures. Documentation must note referrals for action, if any.

Key Issues

- ◆ How will entities publicize complaint procedures to staff and others?
- ◆ What is the most efficient way to handle complaints—one person or several?
- ◆ Should a timeframe for handling complaints exist?
- ◆ Who should be allowed to access complaint information?
- ◆ Who will investigate and resolve complaints and to whom will this person report resolution status?
- ◆ How will this information be maintained, stored, and retrieved? Is there an existing information system that can be used for complaint maintenance?
- ◆ How can entities use complaints to evaluate, improve, or change policies and practices?
- ◆ Will entities use existing complaint processes for information privacy complaints or develop a different process?
- ◆ Should this policy be coordinated with the covered entity's Patient Rights policy?

Category I Guidelines-Actions must be taken to address these

- ◆ Identify a contact person or office to receive complaints about policies and procedures and compliance with them.
- ◆ Maintain a record of complaints and brief explanations of their resolution.

Category II Guidelines-Actions should be taken to address these

- ◆ Determine whether the person or office identified to receive complaints will handle them personally or triage them for handling by others.
- ◆ Determine timeframes and protocols for handling and reporting complaints.
- ◆ Use complaints as evaluative and improvement tools where appropriate.
- ◆ Determine who will access complaint information and for what purposes.
- ◆ Specify a method to track complaints.
- ◆ Report periodically on resolutions of complaints.
- ◆ Coordinate this requirement with the covered entity's Patient Rights policy.

AMC/HIPAA Workgroup

Roadblocks

Operational units within an AMC often address patient complaints directly. Relinquishing this practice in favor of a single person or central office may challenge cultural norms.

Comments

This is related to PRIV.49

PRIV.53 Sanctions [§ 164.530\(e\)\(1\)](#)

HIPAA Requirement

Standard: sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of [§ 164.502\(j\)](#) or paragraph (g)(2) of this section.

(2) Implementation specification: documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

AMC Explanation of HIPAA Regulation

A covered entity must apply and document corrective and disciplinary action when a member of its workforce fails to comply with the covered entity's policies and procedures related to this rule.

Key Issues

- ◆ What sanctions will be applied and when? What gradation will be used?
- ◆ Who reviews instances of noncompliance and recommends sanctions?
- ◆ Who is responsible for applying sanctions?
- ◆ Should physicians have different sanctions?

Category I Guidelines-Actions must be taken to address these

- ◆ Develop sanctions against workforce members who fail to comply with the covered entity's privacy policy.
- ◆ Charge an individual or group to review policy and procedural violations and specify corrective and/or disciplinary action.
- ◆ Apply disciplinary action as necessary and appropriate.
- ◆ Document corrective and disciplinary action taken.

Category II Guidelines-Actions should be taken to address these

- ◆ Make sanctions progressive and commensurate with the severity, frequency, and intent of violations.
- ◆ Apply sanctions equitably without regard to an offender's role or position within the covered entity.
- ◆ Include termination of employment or contract relationship and/or criminal prosecution as possible sanctions.
- ◆ Include provision for sanctions in contract and labor agreements.
- ◆ Coordinate sanctions with the covered entity's human resources department.
- ◆ Consider establishing progressive sanctions, such as verbal warning, written warning, up to termination, and determine when progressive sanctions are appropriate.
- ◆ Make workforce members aware of the sanction procedures.

AMC/HIPAA Workgroup

Roadblocks

Different discipline standards for various personnel categories may exist.

Comments

Publicizing the use of sanctions may be an effective deterrent to misbehavior. The sanctions do not apply to whistleblower activities that meet the provisions of § 164.502(j) or complaints, investigations, or opposition that meet the provisions of § 164.530(g)(2). Business associates are not included under this particular requirement; requirements for business associates are listed in § 164.504.

PRIV.54 Mitigation [§ 164.530\(f\)](#)

HIPAA Requirement

Standard: mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

AMC Explanation of HIPAA Regulation

Covered entities must take positive action to minimize known harmful effects resulting from the unauthorized use or disclosure of protected health information, and are obligated to correct known instances of harm. Business associates have an obligation to notify the covered entity of any harmful effects they know about.

Key Issues

- ◆ At what point does a harmful effect occur—when protected health information is inappropriately used or disclosed, or when the inappropriate use or disclosure has a tangible negative impact?
- ◆ What reasonable steps should a covered entity should take to mitigate harmful effects?
- ◆ What does “harmful effect” mean in the covered entity and how does the entity become aware that one has occurred?

Category I Guidelines-Actions must be taken to address these

- ◆ Minimize harmful effects resulting from unauthorized use or disclosure of protected health information by:
 - ▶ Containing the damage and stopping further compromise; and
 - ▶ Informing those responsible for the policy or procedural breach to prevent future actions that would have harmful effects.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider whether inappropriate use or disclosure may in itself constitute a harmful effect. (This is a legal issue. See Comments.)
- ◆ Consider notifying individuals if misuse or inappropriate disclosure of their protected health information will likely lead to a harmful effect.
- ◆ Include contract language to transfer the potential financial burden of harm to business associates.

Roadblocks

The point at which harmful effects occur is debatable. Notifying patients of inappropriate use or disclosure of protected health information may, at times, cause more grief and consternation than the direct effects of compromised information.

AMC/HIPAA Workgroup

Comments

The rule uses the term *harmful effect* rather than *harm*. This implies something *following* a cause or agent, such as a compromise of information. Inappropriate use or disclosure of protected health information may not be a harmful effect in and of itself.

AMC/HIPAA Workgroup

PRIV.55 Refraining from intimidating or retaliatory acts [§ 164.530\(g\)](#)

HIPAA Requirement

Standard: refraining from intimidating or retaliatory acts. A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

- (1) Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;*
- (2) Individuals and others. Any individual or other person for:*
 - (i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;*
 - (ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or*
 - (iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.*

AMC Explanation of HIPAA Regulation

Covered entities must not retaliate against persons for filing complaints, for testifying, for participating in investigations, compliance reviews, proceedings or hearings, or for opposing real or perceived unlawful acts or practices under this act provided the oppositions are made in good faith.

Key Issues

- ◆ Who will determine the proper response, if any?
- ◆ What will the covered entity do if a workforce member does retaliate?
- ◆ How can one determine whether retaliation is occurring?
- ◆ Is there a monitoring or reporting issue here?
- ◆ How would supervisors know if workforce members are engaged in retaliatory activities?

Category I Guidelines-Actions must be taken to address these

- ◆ Establish policies and procedures that prohibit intimidation, threats, coercion, discrimination, or retaliatory action against individuals who exercise their rights under this act.

Category II Guidelines-Actions should be taken to address these

- ◆ Communicate the non-retaliation policy through related policies and programs (e.g. Standards of Conduct, Mutual Respect, and/or the Integrity Program).
- ◆ Consider reporting mechanisms that protect complainers against retaliation (e.g., removing complainants' identifying information from complaint reports).
- ◆ Coordinate with human resources and labor relations representatives.

AMC/HIPAA Workgroup

Roadblocks

Training will be required to help workforce members to understand what is legal and illegal under HIPAA so that they will correctly recognize illegality outside of their normal scope of operations.

Comments

Communicating the expectations of this standard is critical.

AMC/HIPAA Workgroup

PRIV.56 Waiver of rights [§ 164.530\(h\)](#)

HIPAA Requirement

Standard: Waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

AMC Explanation of HIPAA Regulation

A covered entity may not require individuals to waive their rights to file a complaint or their other rights under the privacy standards as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits. “This subpart” in the regulation text refers to § 164 Subpart E, consisting of §§ 164.500 through 164.534.

Key Issues

- ◆ Should the entity ask patients to voluntarily waive their rights under this rule?

Category I Guidelines-Actions must be taken to address these

- ◆ Do not require individuals to waive their rights to file a complaint or their other rights under the privacy standards as a condition of treatment, payment, and enrollment in a health plan or eligibility for benefits.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider not putting waivers of rights on consent forms.
- ◆ Covered entities should not ask patients to waive their privacy rights.

Roadblocks

No roadblocks specific to this point.

Comments

This requirement ensures that covered entities do not force individuals to give up the rights they have been provided in the privacy standards.

AMC/HIPAA Workgroup

PRIV.57 Policies and procedures [§ 164.530\(i\)\(1\)](#)

HIPAA Requirement

Standard: policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. . The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

AMC Explanation of HIPAA Regulation

A covered entity must create and implement its privacy-related policy and procedure set. Merely having a policy/procedure is not adequate; the design of the policy/procedure set must take into account the size and type of operations in the covered entity.

Key Issues

- ◆ How do the size and type of operations affect the policy/procedure set that must be implemented?
- ◆ How will the covered entity determine what is reasonable in implementing policy/procedure?

Category I Guidelines-Actions must be taken to address these

- ◆ Implement a reasonable policy/procedure set given the covered entity's size and type of operations. (Group health plans that operate as described in §164.530(k) need not conform to this requirement.)

Category II Guidelines-Actions should be taken to address these

- ◆ Formally determine how the covered entity's size and type affect its required policy/procedure creation and implementation process.

Roadblocks

When smaller entities are absorbed by acquisition or merger into larger ones (e.g., an AMC buying a community hospital), the policy/procedure set of the previously small covered entity may not be adequate for its new role as part of the larger covered entity.

Comments

See GEN.06.

PRIV.58 Changes to policies or procedures [§ 164.530\(i\)\(2\)](#)

HIPAA Requirement

Standard: changes to policies or procedures. (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in [§ 164.520](#), and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with [§ 164.520\(b\)\(1\)\(v\)\(C\)](#), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) Implementation specification: changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by [§ 164.520](#), the covered entity must promptly make the appropriate revisions to the notice in accordance with [§ 164.520\(b\)\(3\)](#). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) Implementation specifications: changes to privacy practices stated in the notice. (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by [§ 164.520\(b\)\(3\)](#) to state the changed practice and make the revised notice available as required by [§ 164.520\(c\)](#). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under [§ 164.520\(b\)\(1\)\(v\)\(C\)](#) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation the requirements in paragraphs (i)(4)(i)(A)-(C) of this section; and

AMC/HIPAA Workgroup

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) Implementation specification: changes to other policies or procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

AMC Explanation of HIPAA Regulation

When a change in law affects a covered entity's privacy policy, the policy must change to accommodate the change in law. If the covered entity reserved the right to change its privacy policies and procedures in its privacy notice, it may apply the new standards to protected health information acquired before the change. If it did not, it must continue to apply the old standard to that information. Entities must maintain documentation of their policies and procedures. Note that group health plans are excepted from this requirement (§ 164.530(i)) if they handle little protected health information as described in § 164.530(k).

Key Issues

- ◆ What are the implications on operations of not reserving the right to change policy in the privacy notice, changing it, and then having prior protected health information governed by the old notice and new governed by the new notice?
- ◆ How will the covered entity determine what is reasonable in implementing policy/procedure change?

Category I Guidelines-Actions must be taken to address these

- ◆ Change policies and procedures when changes to law or regulations require it.
- ◆ If the privacy notice provides for changes, change it when policies that affect it change. The new notice will either cover all protected health information, or only new information, depending on whether the prior notice reserved the right to change.
- ◆ Document the policy and procedure change process, either in writing or electronically.

Category II Guidelines-Actions should be taken to address these

- ◆ Consider reserving the right to change privacy policy in the privacy notice.
- ◆ Consider the logistics and communications issues of changes when crafting privacy policies and notices—to employees as well as patients.
- ◆ Determine how covered entity size, complexity, and type affect the policy/procedure creation and implementation process.

Roadblocks

When smaller entities are absorbed by acquisition or merger into larger ones (e.g., an AMC buying a community hospital), the policy/procedure set of the previously small covered entity may not be adequate for its new role as part of the large covered entity.

AMC/HIPAA Workgroup

Comments.

Group health plans that operate as described in § 164.530(k) need not conform to this requirement.

HIPAA Requirement

(1) Standard: Documentation. A covered entity must:

- (i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;*
- (ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and*
- (iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.*

(2) Implementation specification: Retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

AMC Explanation of HIPAA Regulation

This requirement calls for documentation in support of policies and procedures and all other subparts of the privacy regulations that directly list documentation as a requirement. Documentation must be kept current to reflect changes in regulatory requirements and a covered entity's privacy processes, and must be retained for a period of 6 years. It appears that the provisions of this section apply to all of the other documentation requirements of the regulation.

Key Issues

- ◆ How will the entity ensure compliance with document management requirements?
- ◆ How will the entity ensure consistent documentation practices across departments?
- ◆ Who will be allowed to have access to this documentation.

Category I Guidelines-Actions must be taken to address these.

- ◆ Document privacy policies and procedures in written or electronic form.
- ◆ Document required communications, designations, actions, and activities.
- ◆ Record date of creation and last date of effectiveness of documents.
- ◆ Maintain required documentation for six years from date of creation or the date when the policy or procedure was last in effect, whichever is later.

Category II Guidelines-Actions should be taken to address these.

- ◆ Promulgate the policy on documentation from the highest organizational level.
- ◆ Clearly delineate responsibility for documentation of policies and procedures.
- ◆ Specify the rescission and review dates for documentation.
- ◆ Centralize retention of policy and procedure documentation.
- ◆ Communicate to managers that a lack of documentation may be interpreted as failure of compliance.
- ◆ Organize documentation in such a way that it can be identified when necessary.
- ◆ Centralize and standardize documentation across the organization so that it is easily accessible.

AMC/HIPAA Workgroup

Roadblocks

It may be difficult to get some groups within the entity to adopt required documentation practices and procedures. Without direction and accountability for the periodic review and communication of documentation updates, it is easy for documentation to fall by the wayside.

Comments

Several other standards also require documentation of policy and procedure, as well as documentation of consideration given to policies that might not be adopted. Among those are standards associated with JCAHO, the FDA Safe Medical Device Act, OSHA, and others.

Document management could involve a central office, or could be the responsibility of each manager.

AMC/HIPAA Workgroup

General Policy and Management Guidelines

GEN.01 Roles and Responsibilities in Development and Maintenance

AMC Explanation of Guideline

The HIPAA security and privacy regulations include not only explicit requirements for roles but also requirements for activities that imply the creation of formal roles and responsibilities for many people in an institution as large and complex as an AMC. The requirements for a Security Office(r) and a Privacy Official are the starting points, with other bodies needed to serve in developing and maintaining HIPAA compliance elements. Paying careful attention to how roles and responsibilities in developing and maintaining HIPAA compliance are arranged will reduce the amount of waste, confusion, and delay. This section offers some guidance that AMCs may find useful in approaching this subject.

Key Issues

- ◆ How are authority and responsibility for compliance allocated?
- ◆ Who (person and/or unit) is responsible for which aspects of developing the HIPAA program?
- ◆ How can the HIPAA responsibilities be coordinated with the existing management and funding model in the covered entity?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish a formal HIPAA security and privacy compliance program.
- ◆ Enlist external consultants.
- ◆ Push responsibility down to line management.
- ◆ Designate a responsible executive.
- ◆ The coordinator should cultivate a small, informal group of advisors from among those people whose current roles give them a significant stake in how the HIPAA development process is structured (e.g. risk managers, internal auditors, accreditation managers, health information managers, senior IT managers, senior clinical operations managers, counsel).
- ◆ Appoint a Security Officer and a Privacy Official after the awareness phase for senior and middle managers is mature.
- ◆ Require regular reporting to senior management on the status of the development effort during the awareness phase. Continue with a reporting format appropriate to the planning and execution phases.
- ◆ Organize around the idea that HIPAA is a compliance project with strong implications for clinical operations, IT activities, and business relations. Appointments and processes should respect this concept.
- ◆ Establish a set of guidelines for use by the covered entity's management in forming HIPAA-compliant operations. Use these as a common reference in decision-making related to HIPAA.

AMC/HIPAA Workgroup

- ◆ Develop the HIPAA program models that include managers' involvement in ways that will aid each manager's role with HIPAA. Be sure to actively involve managers from the research, education, and clinical care areas of the covered entity.

Roadblocks

Getting enough of the "attention budget" of the key managers may be difficult. Many people in such positions in healthcare today already have full agendas, and making room for HIPAA will likely require adjustment. Also, making costs to meet the HIPAA requirements understandable will require creativity and patience. Credible plans (including resource needs) take the time and attention of managers to create and communicate. Finally, creating a well-timed development effort to comply with the regulations within the time allowed (2 years) could present difficulties for unprepared AMCs.

Comments

None.

GEN.02 Organizational Support for HIPAA Security and Privacy Compliance

This point addresses how to build support for HIPAA security and privacy compliance among line management, who will have to balance compliance activities with many other demands on their time, attention, and resources.

Key Issues

- ◆ What incentives and support for HIPAA compliance activities will be provided to line management whose staff are responsible for handling protected health information or documentation of compliance activities?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Demonstrate executive management commitment to compliance with the HIPAA security and privacy requirements.
- ◆ Provide a contact who can assist line management with compliance activities.
- ◆ Implement accountability for failure to participate in compliance activities.
- ◆ Establish a HIPAA security and privacy compliance reporting program; require compliance reporting on a regular basis.
- ◆ Educate line management on the importance of HIPAA security and privacy compliance, executive management's commitment to compliance, and the consequences of non-compliance. Consider tracking participation in this education program.
- ◆ Include HIPAA security and privacy compliance in line management performance criteria.
- ◆ Establish and publicize sanctions for failing to participate in compliance activities.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

GEN.03 Resources for Development and Maintenance

This point addresses funding of the development and maintenance of a HIPAA Security and Privacy program. While it may be difficult to determine the exact costs of HIPAA security and privacy compliance, resource requirements are likely to be extensive. As an unfunded mandate, it may be difficult to establish appropriate financial and personnel resources.

Key Issues

- ◆ How much will HIPAA security and privacy compliance cost? Determining this will be important for budgeting.
- ◆ How does one go about involving the right people in developing a useful estimate?
- ◆ How should covered entities get started with building HIPAA security and privacy items into the regular operations budget?
- ◆ Who must answer the resource allocation question? Senior executives, boards, etc.?
- ◆ Consider other benefits of compliance.

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Use existing resources to scope effort and cost.
- ◆ Use an incremental funding model.
- ◆ Pay attention to the principles of reasonability and scalability when forming budget estimates.
- ◆ Investigate minimal compliance.
- ◆ Investigate cost recovery specific to the regulatory mandate.
- ◆ Consider non-monetary costs.
- ◆ Compare with the cost of non-compliance, including non-monetary costs.
- ◆ Treat HIPAA security and privacy resource requests as part of the normal budget process.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

GEN.04 Evaluation and Monitoring of Development and Maintenance

This point addresses the development and maintenance of an effective HIPAA security and privacy program. Evaluation and monitoring of compliance activities is a normal feature of any compliance program. To be effective, a covered entity's HIPAA security and privacy compliance program must fit the entity's culture, business operations, and risk management strategy.

Key Issues

- ◆ How can a covered entity make the initial and ongoing compliance activity effective?
- ◆ How will a covered entity formulate a process that evaluates the approach of each unit for adequacy and timeliness? Against what norms should approaches be evaluated?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Establish a governing body for evaluation and monitoring, to guide implementation, and to review compliance.
- ◆ Provide consistent guidelines for HIPAA security and privacy compliance across the covered entity.
- ◆ Forward progress reports up the covered entity's management chain.
- ◆ Formally recognize when work moves from "development" to "operations."
- ◆ Make line executives responsible for compliance oversight.
- ◆ Tie compliance to formal audit and/or accreditation processes.
- ◆ Consider the use of an automated tool to capture compliance activity.***Roadblocks***

No roadblocks specific to this point.

Comments

The reporting technique should define mechanisms to ensure accountability.

AMC/HIPAA Workgroup

GEN.05 Reasonableness

This point addresses how a covered entity can interpret the reasonableness provisions of the HIPAA Security and Privacy regulations. The regulations permit entities to interpret their requirements based on “reasonableness.” Covered entities must exercise judgment to decide what is and is not reasonable. Whether a particular proposed action would be considered reasonable will depend on a number of factors including the nature and size of a covered entity, the covered entity’s internal expertise and technical abilities, the feasibility and difficulty of the proposed action, and the cost of the proposed action.

Key Issues

- ◆ Who in a covered entity will determine what is reasonable for the covered entity?
- ◆ What criteria will be used to judge reasonableness?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Use cost and feasibility studies to assess reasonableness.
- ◆ Conduct risk analysis to assess the reasonableness of compliance measures.
- ◆ Benchmark against similar covered entities and network with peers.
- ◆ Obtain advice of counsel on policies and procedures.
- ◆ Evaluate and monitor functions to ensure the reasonableness of compliance measures.
- ◆ Encourage internal consistency of practices.
- ◆ Document justifications of reasonableness decisions.
- ◆ Establish an effective remedial action process; such a process may be considered evidence of reasonableness.
- ◆ Obtain certification of security procedures; doing so may be considered evidence of reasonableness.

Roadblocks

No roadblocks specific to this point.

Comments

The reasonableness criterion does not appear to apply to unambiguous mandates of the HIPAA Security and Privacy regulations. All of the Category I guidelines in this document represent unambiguous mandates of the regulations, so failing to implement Category I guidelines would likely be considered unreasonable.

AMC/HIPAA Workgroup

GEN.06 Scalability

This point addresses appropriate scaling of each covered entity's HIPAA security and privacy program to its needs. The HIPAA regulations do not take a "one-size fits all" approach; instead, each covered entity is expected to implement provisions of the act in a fashion appropriate to its size and physical environment. What may be an appropriate mechanism for one covered entity may be "overkill" in another.

Key Issues

- ◆ Is the compliance program appropriate to the size of the covered entity?
- ◆ What is reasonable for what size?
- ◆ What physical environment aspects need to be considered?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Tie the justification of selected practices and safeguards to risk analysis.
- ◆ Define your covered entity, its boundaries, and its scope.
- ◆ Consider organizational size, assets, and capabilities in determining the reasonableness of proposals for meeting the HIPAA security and privacy program.
- ◆ Benchmark recommendations of risk analysis efforts against peers.

Comments

Very little guidance is given as to what is reasonable for a given size of covered entity.

GEN.07 Limiting Liability Arising from Compliance

This point addresses procedures for reducing liability associated with information discovered during HIPAA security and privacy compliance activities. During compliance activities, a covered entity may discover information that could create liability. Covered entities should consider taking actions to reduce any such liability, and should consider a variety of mechanisms for reducing these liabilities.

Key Issues

- ◆ What kinds of compliance actions and findings might create liability for the covered entity?
- ◆ Which structures and policies should be used to limit liability arising from compliance activities?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Formulate liability mitigation procedures for internal audit and critical self-analysis findings.
- ◆ Consider the use of attorney-client and other privileges to reduce liability.
- ◆ Document and follow effective problem correction procedures.
- ◆ Benchmark industry best practice and regulatory standards to establish conformance to standards of best practice and due care.
- ◆ Use a formal compliance program as a mitigating factor.
- ◆ Document timeliness of response to reported problems as a mitigating factor.
- ◆ Consider whether certification of the covered entity's security system is a mitigating factor.
- ◆ Involve the covered entity's legal counsel in the design of liability reduction measures.
- ◆ Use the security system to protect the confidentiality of information that might create liability.
- ◆ Review IRB processes in relation to privacy and security incidents.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

GEN.08 HIPAA Accreditation Intersections

This guideline addresses mitigation of inconsistent accreditation requirements. Various independent accrediting bodies such as JCAHO, the College of American Pathologists, Residency Review Committees, state legislation, etc., establish accreditation requirements. These requirements may be internally consistent within each body, but levy inconsistent requirements when viewed in their entirety.

Key Issues

- ◆ How many sets of rules apply to each situation? Which ones?
- ◆ Are these rules consistent? If not, what can be done about the inconsistencies?
- ◆ Do “special” restrictive disorders (psychiatric, HIV, etc.) require “special” permission, which will impair the flow of protected health information between PCPs and specialists?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Compile a comparison list of conflicting rules.
- ◆ Encourage boards, joint commissions, etc., to take public positions on conflicts and eliminate them.
- ◆ Determine whether HIPAA compliance eliminates the need for compliance to some other regimes.
- ◆ Encourage development of reciprocity agreements among regimes.

Comments

The list of private accrediting agencies is quite long. All request that AMCs provide lists of protected health information to do their accreditation work. The AAMC has requested that this requirement be eliminated.

HIPAA Requirement

General rule. A standard, requirement, or implementation specification adopted under or pursuant to this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except where one or more of the following conditions is met:

(a) A determination is made by the Secretary pursuant to § 160.204(a) that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse;

(ii) To ensure appropriate State regulation of insurance and health plans;

(iii) For State reporting on health care delivery or costs; or

(iv) For other purposes related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system; or

(2) Addresses controlled substances.

(b) The provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, or the State established procedures, are established under a State law providing for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

AMC Explanation of HIPAA Regulation

HIPAA's privacy rule is a floor above which more stringent state law applies. HIPAA's security rule, on the other hand, supersedes conflicting state law.

Key Issues

- ◆ What is the process to determine which is the more strict interpretation, state law or the HIPAA privacy regulations?
- ◆ Which law/regulation applies when health care or health plan business is delivered across state lines?
- ◆ How will covered entities that do business in multiple states accommodate the different stricter standards in each state?
- ◆ When does the state of the patient, as opposed to the state of the covered entity, govern which state's laws apply?

AMC/HIPAA Workgroup

Category I Guidelines-Actions must be taken to address these

- ◆ Determine when the federal floor for a particular situation is superseded by state law or regulation.

Category II Guidelines-Actions should be taken to address these

- ◆ Participate in statewide consortia that will provide guidance on when the federal floor for a particular regulation is superseded by state law or regulation. This is an opportunity to build consensus and reduce uncertainty and confusion while constraining costs.
- ◆ Obtain advice from counsel when there are potential issues related to the application of state law.

Roadblocks

Areas of potential conflict between federal and state laws and regulations are a particular problem when the regulations are not written clearly or the interpretation of the regulations is open. Covered entities may need to retain outside counsel to determine specific courses of action.

Comments

State entities are encouraged to proactively request opinions from their state's Attorney General, as well as from state elected officials sponsoring legislation perceived as potentially conflicting.

The following sections may require consideration for potentially more restrictive state law:

- PRIV.11 Right of an individual to request restriction of uses and disclosures § 164.522(a)(1)
- PRIV.24 Uses and disclosures of protected health information for marketing
- PRIV.27 Uses and disclosures required by law § 164.512(a)
- PRIV.29 Disclosures about victims of abuse, neglect or domestic violence § 164.512(c)
- PRIV.31 Disclosures for judicial and administrative proceedings § 164.512(e)
- PRIV.37 Uses and disclosures for specialized government functions § 164.512(k)
- PRIV.58 Changes to policies or procedures § 164.530(i)(2)

For example, consider a situation where a health plan is incorporated in Washington, D.C., a clinic is across the Potomac river in Virginia, and the patient resides in Maryland. There may be conflicting state laws and regulations. How will these be resolved? Likely HIPAA transactions that would cross state borders include enrollment, eligibility, referral and authorization, claim, claim status, and remittance. Additionally, health records may be transferred across state lines in support of care.

GEN.10 Policy establishment and modification

This point addresses the difficulty of establishing consistent policy across a complex covered entity such as an AMC. A covered entity may not have the authority to dictate policies and procedures to some of its subsidiary or affiliate entities. Nevertheless, the covered entity will have to ensure that some of these entities comply with the HIPAA security and privacy requirements.

Key Issues

- ◆ Who (if anyone) has the authority to formulate and implement security and privacy policies for the whole covered entity?
- ◆ If subsidiary or affiliate entities have independent policy formulation processes, how can the covered entity influence these entities to comply with HIPAA security and privacy requirements in a consistent way?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Choose the covered entity's structure and affiliate relationships carefully where flexibility in defining covered entity structure exists.
- ◆ Encourage independent policy formulation authorities to work together on HIPAA security and privacy policy development and implementation.
- ◆ Use existing policy formulation and implementation processes and agreements wherever possible (human resources processes, union contracts, etc.).
- ◆ Consider requiring specific policies and procedures in contracts if necessary.

Roadblocks

No roadblocks specific to this point.

Comments

None.

GEN.11 Policy Usage Introduction

This point addresses strategies for successfully introducing HIPAA security and privacy policies and procedures. Covered entities need to ensure that their employees learn and follow newly introduced HIPAA security and privacy policies.

Key Issues

- ◆ What factors contribute to successful introduction of new security and privacy policies?
- ◆ What models for successful policy introduction already exist within the covered entity?
- ◆ To what extent will acceptance be dependent on the degree of change mandated and the methods used to elicit compliance?
- ◆ What are the consequences if HIPAA security and privacy policies are not consistently observed?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Justify policies by explaining how they benefit the covered entity and its customers.
- ◆ Emphasize the risks of non-compliance.
- ◆ Model security and privacy policy deployments on previous successful policy deployments within the covered entity. Look specifically at human resources policy introduction processes.
- ◆ Require and keep records of workforce members' acknowledgement that they have received and understood security and privacy policy.
- ◆ Examine policy compliance during risk assessment and accreditation; implement corrective actions if necessary.
- ◆ Consider pilot policy deployments and adjust broader deployment plans based on the results of the pilots.

Roadblocks

No roadblocks specific to this point.

Comments

None.

AMC/HIPAA Workgroup

GEN.12 Privacy Culture

This guideline addresses the fostering of cultural changes through the creation of a privacy culture. Privacy culture changes are often shaped by societal expectations resulting from law, regulation, and litigation. Compliance with the HIPAA privacy regulations carries with it a need to change the accountability and responsibility for privacy within a covered entity. This process of change is facilitated through an appreciation of the sensitivity of the data being handled. In addition, the security regulations will serve as a tool to enable the protection of privacy.

Key Issues

- ◆ How can a covered entity change workforce members' existing bad habits in using and communicating information?
- ◆ How will a covered entity adapt to societal expectations related to privacy?
- ◆ How long will it take to change the current culture; how can a covered entity assess/measure it?
- ◆ Are there issues of institutional conformity in a multi-facility covered entity?
- ◆ How can covered entities induce the same level of regard for privacy within associated entities and business partners?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Have senior management set clear expectations.
- ◆ Ensure that role models set a good example.
- ◆ Provide feedback on security and privacy behavior.
- ◆ Publicize the application of sanctions.
- ◆ Incorporate consumer perceptions, expectations, and suggestions into the curriculum.
- ◆ Hold collegial discussions.
- ◆ Incorporate security and privacy in the curriculum (to build good habits early).
- ◆ Provide orientation training in terms of the expected culture of privacy, and establish and enforce policies dealing with transgressions.

Roadblocks

Implementing the HIPAA security and privacy regulations will require a culture change with regard to how patient information is handled in most AMCs. Developing a program to induce this culture change requires support from senior managers, funding, elapsed time, and staff time from a significant percentage of the staff in the AMC. Each of the early developmental choices in HIPAA must work with this set of circumstances to achieve this type of change.

Comments

None.

GEN.13 Digital Signature

This guideline addresses digital signature mechanisms and standards employed with respect to HIPAA identified transactions.

HIPAA Requirement

PL 104-91 Sec. 11173 (e) Electronic Signature.

(1) Standards. The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1).

(2) Effect of Compliance. Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

Section 1173 (a)

(1) In General. The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for--

(A) the financial and administrative transactions described in paragraph (2); and Other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

AMC Explanation

The final DHHS Security rule may or may not contain the Secretary's response to HIPAA's electronic signature requirements. This is due to the fact that suitable standards for digital signatures in healthcare (as published by an ANSI accredited standards development organization) currently do not exist. Nevertheless, it is anticipated that an electronic/digital signature rule will ultimately be provided in response to HIPAA legislation — if not in the security rule itself, then later on as a new rule.

In accordance with the draft DHHS Security and Electronic Signature Proposed Rule [45 CFR 160], if an electronic signature is required, then it must be a digital signature. When one of the required standard claims transactions uses a digital signature (none of the current transactions are required to at present), the digital signature *must* provide:

- d) Message integrity;
- e) Non-repudiation;
- f) User authentication; and
- g) Proof of "intent" to sign.

The digital signature *may* also provide:

AMC/HIPAA Workgroup

- h) Ability to add attributes;
- i) Continuity of signature capability;
- j) Countersignature capability;
- k) Independent verifiability;
- l) Interoperability;
- m) Multiple signatures; and
- n) Transportability.

Key Issues,

- ◆ When must a digital signature be used?
- ◆ How and when should a covered entity gain access to a suitable Public Key Infrastructure (PKI)?

Category I Guidelines-Actions must be taken to address these.

None; this section is advisory only.

Category II Guidelines-Actions should be taken to address these

- ◆ Anticipate and plan for participation in a PKI.
- ◆ Actively follow and participate in the development of digital signature standards through ANSI HISB and ANSI accredited standards development organizations.
- ◆ Plan for, budget for, and educate workforce members on the technology and use of digital signatures.
- ◆ Plan for, and adopt/develop certificate policies for, PKI and digital signatures. These policies should include granting, suspending, and revoking certificates, and assuring interoperability.
- ◆ Plan to replace proprietary electronic signatures with an interoperable standards-based digital signature.
- ◆ Consider developing limited near-term digital signature pilots.

Roadblocks

The technology of public key infrastructures and digital signatures is still relatively new, expensive, and may not be suitable for small covered entities. A cost-benefit analysis may be appropriate.

Replacing proprietary electronic signatures with a digital signature may require significant changes to heritage healthcare applications. Electronic signatures developed as part of a healthcare application reside on the application server. Digital signatures, on the other hand, are bound to end users who retain control of their own private keys. Therefore, digital signatures are associated with the end user device, the server functioning to securely store the signed documents/transactions.

Comments

Standards development organizations (SDO) including NCPDP, X12, ASTM, HLT, and W3C met in Orlando, Florida on 8 January 2001 and agreed to the development of a Multi-SDO Digital Signature Standard. The standard would be largely based on standards work recently approved from ASTM and HL7. Subsequently, hearings were held with NCVHS. ANSI HISB

AMC/HIPAA Workgroup

will act to coordinate the development with the goal of producing the standard in the latter part of 2001.

Draft certificate policies are under development by the NIST sponsored Federal PKI Technical Working Group and from ASTM.

Further information on the Multi-SDO Digital Signature Project is available at:
<http://hl7.org/special/Committees/multiSDO/index.htm>

References:

The following digital signature standards in healthcare are germane:

- o) ASTM E1762-95 Standard Guide for Electronic Authentication of Health Care Information
- p) ASTM E2084-00 Standard Specification for Authentication of Healthcare Information Using Digital Signatures
- q) ASTM E2085-00a Standard Guide on Security Framework for Healthcare Information
- r) HL7 Version 3.0

AMC/HIPAA Workgroup

GEN.14 Other Federal Law and HIPAA Privacy

HIPAA's Privacy provisions interact with related provisions in several other federal laws. Those most likely to be of primary interest to AMCs are discussed below.

Key Issues

- ◆ How do the interactions with the various relevant federal laws affect the policy, procedure, and practice set in the AMC?
- ◆ What protections will be provided for student records in a student health clinic of the AMC?
- ◆ How will HIPAA coverage of ERISA-based plans affect AMC health plan operations?
- ◆ How will the operational resources who work with FERPA, non-FERPA, and HIPAA health records manage privacy issues?
- ◆ How will the interactions between CLIA (Clinical Laboratory Improvement Amendments) and HIPAA affect patient access process?
- ◆ How will the safe harbor provisions related to the European Union privacy directive affect CROs?

Category I Guidelines-Actions must be taken to address these.

- ◆ Align the AMC's privacy program to be consistent with the intersecting demands of other federal laws related to privacy practices.

Category II Guidelines-Actions should be taken to address these

- ◆ AMCs should ensure that the program managers in the areas affected by the intersecting (e.g. the Benefits group that handles the ERISA plan) are part of the HIPAA program team.
- ◆ AMCs should consider offering protections that comply with FERPA and HIPAA, even where not required to do so, to student health records within the student health clinics, educational administration, and other clinical facilities (e.g. the AMC's local hospital). Doing so will avoid having to interface multiple protection standards for the same person and sometimes even the same episode of care.
- ◆ AMCs should seek advice from their legal counsels with respect to these intersecting laws.

Roadblocks

No roadblocks specific to this point.

Comments

HIPAA Privacy provisions interact with several other Federal laws and at least one international agreement. The preamble of the privacy rule discusses the following laws and their interactions with HIPAA:

- The Privacy Act;
- The Freedom of Information Act;
- Federal Substance Abuse Confidentiality Requirements;

AMC/HIPAA Workgroup

- Employee Retirement Income Security Act of 1974;
- The Family Educational Rights and Privacy Act;
- Gramm-Leach-Bliley;
- Federally Funded Health Programs;
- Food, Drug, and Cosmetic Act;
- Clinical Laboratory Improvement Amendments;
- Other Mandatory Federal or State Laws;
- Federal Disability Nondiscrimination Laws; and
- U.S. Safe Harbor Privacy Principles (European Union Directive on Data Protection).

The laws most likely to be of interest to AMCs are noted below:

Employee Retirement Income Security Act of 1974

HIPAA does cover the ERISA plans in the typical AMC. There do not appear to be any serious interactions between HIPAA privacy and ERISA

The Family Educational Rights and Privacy Act (FERPA)-

FERPA covers educational records in K-12 and post-secondary institutions that receive Federal funds.

- In FERPA-covered post-secondary institutions the records that are in the typical student health clinic *are not* considered FERPA educational records. Records shared for purposes other than treatment (e.g. immunization declarations for dorm placement) in these settings *are* FERPA educational records.
- The non-FERPA health records are also specifically *excluded* from HIPAA Privacy rule coverage by the definition of “protected health information” in § 164.501 (Definitions). See the discussion in the privacy rule preamble on 20 U.S.C. §1232g(a)(4)(B)(iv).
- The implication for the typical AMC is that the typical records in the student health center are not covered by HIPAA or FERPA. AMCs will therefore only be required to provide privacy measures required by other laws, regulations, and/or accreditation standards.

Federally Funded Health Programs

AMCs do a great deal of business with federally funded health plans (e.g. Medicare, Medicaid, CHAMPUS). These plans were specifically included in HIPAA coverage as “health plans” by the HIPAA law.

Food, Drug, and Cosmetic Act

Many AMCs use products that are either under development or in early release use. Reports on adverse events and related disclosures to the FDA and FDA authorized persons are provided for in HIPAA in § 164.512(b)(1)(iii).

Clinical Laboratory Improvement Amendments

AMC/HIPAA Workgroup

Many AMC labs are governed by CLIA. CLIA requires that test results be provided to authorized persons only. State law defines “authorized person;” it is typically the person who ordered the test. CLIA’s rule will override HIPAA’s requirement that the patient be provided their protected health information by the lab. Since the lab results are almost always reported to a covered entity (e.g. hospital, physician), however, the patient may still gain access to his information through those to whom the lab results have been reported.

U.S. Safe Harbor Privacy Principles (European Union Directive on Data Protection)

Many AMCs engage in worldwide trials of pharmaceuticals, some of which include participants in the European Union. The Safe Harbor provisions (on the Department of Commerce web site, <http://www.export.gov/safeharbor/>) allow U.S. organizations that comply with the provisions to receive data on European Union citizens at facilities located within the United States. The general intent evidenced by the U.S. team during the negotiations of the Safe Harbor provisions was to ensure that those entities who were HIPAA compliant would also be within the safe harbor set; however, no declaration or analysis to that effect is available in the HIPAA privacy rule.

AMC/HIPAA Workgroup

Acronyms

Acronym	Description
AAMC	Association of American Medical Colleges
ABA	American Bar Association
AMC	Academic Medical Center
ASTM	American Society for Testing and Materials
BPA	Blanket Purchase Agreement
CAP	College of American Pathologists
CEO	Chief Executive Officer
CIO	Chief Information Officer
CLIA	Clinical Laboratory Improvement Amendments
COT	Chain-of-Trust
CPRI-HOST	Consolidation of Computer-based Patient Record Institute (CPRI) and Healthcare Open Systems and Trials (HOST)
CPU	Central Processing Unit
CRO	Clinical Research Organization
DHHS	Department of Health and Human Services
ERISA	Employee Retirement Income Security Act
FDA	Federal Drug Administration
FERPA	Family Educational Rights and Privacy Act (a.k.a. the Buckley Amendment)
FTE	Full-Time Equivalent
HIM	Health Information Management
HIPAA	Health Information Portability and Accountability Act
IA	Internal Audit
IRB	Institutional Review Board
ISO	International Standards Organization
IT	Information Technology
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
LCME	Liaison Committee on Medical Education
NLM	National Library of Medicine
NPRM	Notice of Proposed Rule Making
OMG	Object Management Group
OSHA	Occupational Safety and Health Administration
PCP	Primary Care Provider
PHI	Protected Health Information
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
RM	Risk Management
SURA	Southeastern Universities Research Association
TACACS	Terminal Access Control Protocol
TPA	Third Party Administrator
WEDI	Workgroup for Electronic Data Interchange

AMC/HIPAA Workgroup

Definitions of Terms Used in this Guideline

Term	Definitions
Access control	<p>The prevention of unauthorized use of a resource. [ISO 7498-2]</p> <p>Information-use policy to determine who can have access to what data/information (both within and external to the organization adopting the access control policy); policies and procedures preventing access by those who are not authorized to have it. [Institute of Medicine, 1994].</p>
Accountability	<p>The property that ensures that the actions of an entity can be traced. [ISO 7498 - 2]</p> <p>The concept that individual persons or entities can be held responsible for specified actions, such as obtaining informed consent or breaching confidentiality. [National Research Council, 1997]</p>
Accreditation	<p>The official management authorization for operation of an MIS. It provides a formal declaration by an Accrediting Authority that a computer system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is based on the certification process as well as other management considerations. An accreditation statement affixes security responsibility with the Accrediting Authority and shows that proper care has been taken for security.</p>
Anonymized data	<p>Identifiers removed and NO means exists for re-identifying patients/subjects.</p>
Anonymous data	<p>Never labeled with patient/subject identifiers</p>
Audit	<p>To record independently and later examine system activity (e.g., logins and logouts, file accesses, security violations). See security audit. [O'Reilly, 1992]</p>
Authentication	<p>The corroboration that an entity is the one claimed. [ISO 7498 - 2].</p> <p>The process of proving that a subject (e.g., a user or a system) is who or what the subject claims to be. Authentication is a measure used to verify the eligibility of a subject to access certain information. It protects against the fraudulent use of a system or the fraudulent transmission of information. There are three classic ways to authenticate yourself: something you know, something you have, or something you are. [O'Reilly, 1992]</p> <p>Providing assurance regarding the identity of subject (author) or object (information). [ASTM 1762] Authentication of data origin is corroboration that the source of data is received as is claimed [ASTM E1762] Authentication of user is the provision of assurance of the claimed identity of an individual or entity [ASTM E1762]</p>
Authorization	<p>The granting of rights, which includes the granting of access based on access rights. [ISO 7498 - 2]</p> <p>The mechanism for obtaining consent for the use and disclosure of health information. The American Health Information Management Association has</p>

AMC/HIPAA Workgroup

Term	Definitions
	<p>recommended requirements for valid authorization. Within the context of a computer-based patient record system, these requirements would include that the authorization be documented (electronically), be addressed to a specific health care provider, specifically identify the patient, identify the individual or entity authorized to receive the information, identify the information that is to be released, specify the purpose for the disclosure, specify under what conditions the authorization will expire unless revoked earlier, indicate that the authorization is subject to revocation, be (electronically) signed by the patient or patient's legal representative, and be dated sometime after the information has been collected. [AHIMA, 1994a]</p>
Biometrics	<p>In computer security, the use of unique, quantifiable physiological, behavioral, and morphological characteristics to provide positive personal identification. Examples of such characteristics are fingerprints, retina patterns, and signatures. [O'Reilly]</p> <p>A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature). [ASTM E1762]</p>
Business Associate	<p>A person (who) performs functions or activities on behalf of, or provides the specified services to or for, an organized health care health care arrangement in which the covered entity participates. A business associate may be a covered entity. The definition of business associate excludes a person who is part of the covered entity's workforce. [45 CFR 160]</p>
Business Partner	<p>A person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform a function or activity for the covered entity. [45 CFR 160]</p>
Cache	<p>A block of memory that holds frequently used data or data that is waiting for another process to use it.</p>
Certification	<p>The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. [O'Reilly, 1992]</p> <p>The administrative act of approving a system for use in a particular application. [National Research Council, 1991]</p>
Chain of trust (partner) agreement	<p>Contract entered into by two business partners in which it is agreed to exchange data and that the first party will transmit information to the second party, where the data transmitted is agreed to be protected between the partners. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple such two-party contracts may be involved in moving information from the originator to the ultimate recipient, for example, a provider may contract with a clearing house to transmit claims to the clearing house; the clearing house, in turn, may contract with another clearing house or with a payer for the further transmittal of those same claims. [45 CFR 142]</p>
Check sum	<p>Numbers summed according to a particular set of rules and used to verify that transmitted data has not been modified during transmission. [O'Reilly, 1992]</p>

AMC/HIPAA Workgroup

Term	Definitions
	Digits or bits summed according to arbitrary rules and used to verify the integrity of data. [National Research Council, 1991]
Confidentiality	<p>A condition in which information is shared or released in a controlled manner. [National Research Council, 1997].</p> <p>The property that information is not made available or disclosed to unauthorized individuals, entities or processes. [ISO 7498 - 2].</p> <p>A security principle that keeps information from being disclosed to any one not authorized to access it. [O'Reilly]</p> <p>The act of limiting disclosure of private matters; maintaining the trust that an individual has placed in one which has been entrusted with private matters. [CPRI, 1995b]</p> <p>The status accorded to data or information indicating that it is sensitive for some reason, and that therefore it needs to be protected against theft or improper use and must be disseminated only to individuals or organizations authorized to have it. [Ball and Collen, 1992; OTA, 1993]</p>
Consent	<p>A consent under this section must be in plain language and:</p> <ol style="list-style-type: none">(1) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment, or health care operations;(2) Refer the individual to the notice required by § 164.520 for a more complete description of such uses and disclosures and state that the individual has the right to review the notice prior to signing the consent;(3) If the covered entity has reserved the right to change its privacy practices that are described in the notice in accordance with § 164.520(b)(1)(v)(C), state that the terms of its notice may change and describe how the individual may obtain a revised notice;(4) State that:<ol style="list-style-type: none">(i) The individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment, or health care operations;(ii) The covered entity is not required to agree to requested restrictions; and(iii) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;(5) State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and(6) Be signed by the individual and dated. [45 CFR 160]
Context based access	An access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external factors" might include time of day, location of the user, strength of user authentication, etc. [45 CFR 142]
Contingency Plan	A plan for responding to a system emergency. The plan includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. Synonymous with disaster recovery plan. [O'Reilly, 1992]
Data Authentication	The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature. [45 CFR 142]

AMC/HIPAA Workgroup

Term	Definitions
Data backup	A retrievable, exact copy of information. [45 CFR 142]
Data Set	A semantically meaningful unit of information exchanged between two parties to a transaction. [45 CFR 162.103]
De-identified data	A record in which identifying information has been removed to render the information de-identified and thus not subject to the rule. [45 CFR 150].
Digital signatures	<p>Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the unit and protect against forgery e.g., by the recipient. [ISO 7498 - 2].</p> <p>An authentication mechanism which enables the creator of a message to attach a code that acts as a signature. The signature guarantees the source and integrity of the message. [Stallings]</p> <p>An authentication tool that verifies the origin of a message and the identity of the sender and receiver. Can be used to resolve any authentication issues between the sender and receiver. A digital signature is unique for every transaction. [O'Reilly, 1992]</p> <p>A means to guarantee the authenticity of a set of input data the same way a written signature verifies the authenticity of a paper document. A cryptographic transformation of data that allows a recipient of the data to prove the source and integrity of the data and protect against forgery. Specifically, an asymmetric cryptographic technique in which each user is associated with a public key distributed to potential verifiers of the user's digital signature used to encrypt messages destined for other users, and a private key known only to the user and is used to decrypt incoming messages. To sign a document, the document and private key are input to a cryptographic process which outputs a bit string (the signature). To verify a signature, the signature, document, and user's public key are input to a cryptographic process, which returns an indication of success for failure. Any modification to the document after it is signed will cause the signature verification to fail (integrity). If the signature was computed using a private key other than the one corresponding to the public key used for verification, the verification will fail (authentication). [ASTM E1762]</p>
Disclosure	The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. [45 CFR 160]
Firewall	A dedicated computer equipped with safeguards that acts as a single, more easily defined, Internet connection [Cheswick and Bellovin, 1994]
Hybrid entity	A single legal entity that is a covered entity and whose covered functions are not its primary functions. [45 CFR 160]
Integrity	<p>The property that data has not been altered or destroyed in an unauthorized manner. [ISO 7498 - 2].</p> <p>A security principle that keeps information from being modified or otherwise corrupted either maliciously or accidentally. Integrity protects against forgery or tampering.[O'Reilly]</p>

AMC/HIPAA Workgroup

Term	Definitions
	<p>The property that an object (health data or information) is modified only in a specified and authorized manner. [Ball and Collen, 1992]</p> <p>Data integrity (the accuracy and completeness of the data) , program integrity, system integrity, and network integrity are all relevant to consideration of computer and system security. [National Research Council, 1991]</p>
Internal Audit	The in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an organization. [45 CFR 142]
Kerberos	The name given to Project Athena's code authentication service. [Stallings, 1995]
Message authentication codes	A code calculated during encryption and appended to a message. If the message authentication code calculated during decryption matches the appended code, the message was not altered during transmission. [O'Reilly, 1992] Sometimes the acronym "MAC" is used for message authentication code.
Minimum Necessary	The "minimum necessary" policy in the final rule has essentially three components: first, it does not pertain to certain uses and disclosures including treatment-related exchange of information among health care providers; second, for disclosures that are made on a routine and recurring basis, such as insurance claims, a covered entity is required to have policies and procedures for governing such exchanges (but the rule does not require a case-by-case determination); and third, providers must have a process for reviewing non-routine requests on a case-by-case basis to assure that only the minimum necessary information is disclosed. [45 CFR 160]
Need to Know Principle	A security principle stating that a user should have access only to the data he or she needs to perform a particular function. (O'Reilly, 1992, as cited in the HISB draft Glossary of Terms
Penetration testing	<p>Penetration testing is a controlled simulation of a "real-world scenario" executed as a comparative assessment to test the protective capability of a system and its resources. As such, penetration testing must have clearly defined strategic and tactical objectives.</p> <p>Strategic Objective: Strategically, the objective of penetration testing is to identify and deploy an ongoing service that provides an informed view, backed up with evidence, that represents the actual state of security of computational facilities, network services, and levels of employee security awareness.</p> <p>Tactical Objective: Tactically, the objective is the identification of infiltration vulnerabilities and the reduction of the associative risk(s) that a penetration team is capable of exploiting.</p>
Personal identification number	<p>A number or code of some kind that is unique to an individual and can be used to provide identity. Often used with automatic teller machines and access devices. [O'Reilly, 1992]</p> <p>Typically used in connection with automated teller machines to authenticate a user. [National Research Council, 1991]</p>
Physical security	Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion.

AMC/HIPAA Workgroup

Term	Definitions
Privacy	<p>Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities. [O'Reilly, 1992]</p> <p>The measures used to provide physical protection of resources against deliberate and accidental threats. [CORBA Security Services, 1997]</p> <p>"The right to be let alone." See L. Brandeis, S. Warren, "The Right To Privacy,"</p> <p>"The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated." See A. Cavoukian, D. Tapscott, "Who Knows: Safeguarding Your Privacy in a Networked World," Random House (1995).</p>
Research	<p>A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. [45 CFR 160]</p>
Risk	<p>The aggregate effect of the likelihood of occurrence of a particular threat with the degree of vulnerability to that threat and the potential consequences of the impact to the organization if the threat did occur. [Stallings, 1995]</p>
Risk management	<p>Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.</p> <p>(NIST Pub. 800-14)</p>
Role	<p>A privilege attribute representing the position or function a user represents in seeking security authentication. A given human being may play multiple roles and therefore require multiple role privilege attributes. [CORBA Security Services, 1997]</p>
Role based access	<p>Role-based access control (RBAC) is an alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. With RBAC, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role. [45 CFR 142]</p>
Safeguards	<p>The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include, but are not necessarily limited to: hardware and software security features; operating procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices. Also called security controls.</p>
Sanction policy	<p>Organizations must have policies and procedures regarding disciplinary actions which are communicated to all employees, agents, and contractors, for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment, and contract penalties (ASTM E 1869)</p> <p>In addition to enterprise sanctions, employees, agents, and contractors must be advised of civil or criminal penalties for misuse or misappropriation of health information. Employees, agents, and contractors must be made aware that</p>

AMC/HIPAA Workgroup

Term	Definitions
	violations may result in notification to law enforcement officials and regulatory, accreditation, and licensure organizations. (ASTM)
Security Policy	<p>The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system. [OTA, 1993]</p> <p>The American Health Information Management Association recommends that security policies apply to all employees, medical staff members, volunteers, students, faculty, independent contractors, and agents. [AHIMA, 1996c] (as cited in HISB, Draft Glossary of Terms Related to Information Security in Health Care Information Systems)</p>
Security testing	A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. This process includes hands-on functional testing, penetration testing, and verification. [Glossary of INFOSEC and INFOSEC Related Terms--Idaho State University]
Technical security mechanism	The processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network. [45 CFR 142]
Technical security services	The processes that are put in place (1) to protect information and (2) to control and monitor individual access to information. [45 CFR 142]
Threat	<p>An action or event that might prejudice security. [ITSEC]</p> <p>A possible danger to a computer system. See also active threat and passive threat. [O'Reilly, 1992]</p> <p>The potential for exploitation of a vulnerability. [National Research Council, 1991]</p>
Tokens	<p>When used in the context of authentication, a physical device necessary for user identification. [National Research Council, 1991]</p> <p>A physical item that is used to provide identity. Typically an electronic device that can be inserted in a door or a computer system to gain access. [O'Reilly, 1992]</p>
Virus	<p>A computer program, typically hidden, that attaches itself to other programs and has the ability to replicate. In personal computers, "viruses" are generally Trojan horse programs that are replicated by inadvertent human action and which, when executed, result in undesired side effects generally unanticipated by the user.</p> <p>A type of programmed threat. A code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users. [O'Reilly, 1992]</p> <p>Code embedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function. [Stallings, 1995]</p>
Vulnerability	A security weakness due to failures in analysis, design, implementation, or

AMC/HIPAA Workgroup

Term	Definitions
	<p>operation. [ITSEC]</p> <p>A weakness in a system that can be exploited to violate the system's intended behavior. There may be security, integrity, availability, and other vulnerabilities. The act of exploiting vulnerability represents a threat, which has an associated risk of being exploited. [National Research Council, 1991]</p>
Workforce	<p>Employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity. [45 CFR 160.103]</p> <p>Any person engaged in providing services, administrative support or direction to those providing services to clients of an Academic Medical Center. This includes employees of the AMC, professional providers who are given professional privileges to practice in the AMC, volunteers, students and professionals engaged in training and supervised under a sanctioned program recognized by the AMC, the Board of Governors and Directors (or analogous body) and executives managing the affairs of the AMC.</p>
Workforce Member	<p>A person belonging to the workforce. Clarified by "If there is no business associate contract, we assume the person is a member of the covered entity's workforce. We note that independent contractors may or may not be workforce members. However, for compliance purposes we will assume that such personnel are members of the workforce if no business associate contract exists." [45 CFR 160] See Workforce.</p>

AMC/HIPAA Workgroup

References

- [45 CFR 142] Department of Health and Human Services, 45 CFR Part 142 Security and Electronic Signature Standards; Proposed Rule, 12 August 1998
- [45 CFR 160] HHS, 45 CFR Parts 160 Through 164: Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, November 3, 1999
- [AHIMA, 1994a] AHIMA, 1994a. Guidelines on Maintenance, Disclosure, and Redisclosure of Health Information. Chicago: American Health Information Management Association.
- [ASTM 1762] ASTM 1762. Guide for Electronic Authentication of Health Care Information. Committee E-31 on Computerized Systems, Subcommittee E31.20 on Authentication. West Conshohocken, PA: ASTM, Oct. 10, 1995.
- [CORBA Security Services, 1996] The Object Management Group, "CORBAservices", OMG Publications, 1996, Chapter 15.
- [CPRI, 1995b] CPRI, 1995b. Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Records. Work Group on Confidentiality, Privacy & Security, Schaumburg, IL: Computer-based Patient Record Institute, February.
- [ISO 7498-2] ISO 7498-2, "Information Processing systems -Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture", International Standards Organization, 1989.
- [Iglehart] Iglehart J. Forum on the future of academic medicine: session IV--the realities of the health care environment Acad Med 1998 73: 956-961.
- [ITSEC] ITSEC "Information Technology Security Evaluation Criteria" European Commission, 1991
- [National Research Council, 1997] National Research Council, "For the Record: Protecting Electronic Health Information", Computer Science and Telecommunications Board, National Academy Press, Washington, DC, 1997.
- [O'Reilly] D. Russell and G.T. Gangemi Sr., "Computer Security Basics", O'Reilly & Associates, Inc., CA, 1996. ISBN 0-937175-71-4.
- "Prescription for Change: Report of the Task Force on Academic Health Centers" The Commonwealth Fund, 1985.
- [Stallings, 1995] W. Stallings, "Network and Internetwork Security Principles and Practice", The Institute of Electrical and Electronic Engineers, Inc., New York, 1995. ISBN 0-02-415483-0.

AMC/HIPAA Workgroup

“What Americans Say about the nation’s medical schools and teaching hospitals” Report on Public Opinion Research. AAMC, 1996.

AMC/HIPAA Workgroup

Privacy Standards Extract

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) Pursuant to and in compliance with a consent that complies with § 164.506, to carry out treatment, payment, or health care operations;

(iii) Without consent, if consent is not required under § 164.506(a) and has not been sought under § 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes;

(iv) Pursuant to and in compliance with an authorization that complies with § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), and (g).

(2) Required disclosures. A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and as required by §§ 164.524 or 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

AMC/HIPAA Workgroup

(b) Standard: minimum necessary. (1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section, as required by paragraph (a)(2)(i) of this section, or pursuant to an authorization under § 164.508, except for authorizations requested by the covered entity under § 164.508(d), (e), or (f);

(iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(iv) Uses or disclosures that are required by law, as described by § 164.512(a);

and

(v) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) Standard: uses and disclosures of protected health information subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) Standard: uses and disclosures of de-identified protected health information.

AMC/HIPAA Workgroup

(1) Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) Uses and disclosures of de-identified information. Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) Standard: disclosures to business associates. (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

AMC/HIPAA Workgroup

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).

(2) Implementation specification: documentation. A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

AMC/HIPAA Workgroup

(f) Standard: deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.

(g)(1) Standard: personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) Implementation specification: adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3) Implementation specification: unemancipated minors. If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has

AMC/HIPAA Workgroup

also been obtained; and the minor has not requested that such person be treated as the personal representative;

(ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

(iii) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(4) Implementation specification: deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) Implementation specification: abuse, neglect, endangerment situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

AMC/HIPAA Workgroup

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) Standard: confidential communications. A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) Standard: uses and disclosures consistent with notice. A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) Standard: disclosures by whistleblowers and workforce member crime victims.

(1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

AMC/HIPAA Workgroup

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

§ 164.504 Uses and disclosures: organizational requirements.

(a) Definitions. As used in this section:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

AMC/HIPAA Workgroup

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Health care component has the following meaning:

(1) Components of a covered entity that perform covered functions are part of the health care component.

(2) Another component of the covered entity is part of the entity's health care component to the extent that:

(i) It performs, with respect to a component that performs covered functions, activities that would make such other component a business associate of the component that performs covered functions if the two components were separate legal entities; and

(ii) The activities involve the use or disclosure of protected health information that such other component creates or receives from or on behalf of the component that performs covered functions.

Hybrid entity means a single legal entity that is a covered entity and whose covered functions are not its primary functions.

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Summary health information means information, that may be individually identifiable health information, and:

AMC/HIPAA Workgroup

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b) Standard: health care component. If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.

(c)(1) Implementation specification: application of other provisions. In applying a provision of this subpart, other than this section, to a hybrid entity:

(i) A reference in such provision to a “covered entity” refers to a health care component of the covered entity;

(ii) A reference in such provision to a “health plan,” “covered health care provider,” or “health care clearinghouse” refers to a health care component of the covered entity if such health care component performs the functions of a health plan, covered health care provider, or health care clearinghouse, as applicable; and

(iii) A reference in such provision to “protected health information” refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.

(2) Implementation specifications: safeguard requirements. The covered entity that is a hybrid entity must ensure that a health care component of the entity complies

AMC/HIPAA Workgroup

with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:

(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(ii) A component that is described by paragraph (2)(i) of the definition of *health care component* in this section does not use or disclose protected health information that is within paragraph (2)(ii) of such definition for purposes of its activities other than those described by paragraph (2)(i) of such definition in a way prohibited by this subpart; and

(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by this subpart.

(3) Implementation specifications: responsibilities of the covered entity. A covered entity that is a hybrid entity has the following responsibilities:

(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply with this subpart.

AMC/HIPAA Workgroup

(ii) The covered entity has the responsibility for complying with § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j).

(d)(1) Standard: affiliated covered entities. Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.

(2) Implementation specifications: requirements for designation of an affiliated covered entity. (i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.

(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).

(3) Implementation specifications: safeguard requirements. An affiliated covered entity must ensure that:

(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and

AMC/HIPAA Workgroup

(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.

(e)(1) Standard: business associate contracts. (i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) Implementation specifications: business associate contracts. A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

AMC/HIPAA Workgroup

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

AMC/HIPAA Workgroup

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) Implementation specifications: other arrangements. (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.

(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.

AMC/HIPAA Workgroup

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of *business associate* in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(4) Implementation specifications: other requirements for contracts and other arrangements. (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

- (A) For the proper management and administration of the business associate; or
- (B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

AMC/HIPAA Workgroup

(A) The disclosure is required by law; or

(B)(I) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f)(1)Standard: requirements for group health plans. (i) Except as provided under paragraph (f)(1)(ii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and discloses of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(2) Implementation specifications: requirements for plan documents. The plan documents of the group health plan must be amended to incorporate provisions to:

AMC/HIPAA Workgroup

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

AMC/HIPAA Workgroup

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

AMC/HIPAA Workgroup

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) Implementation specifications: uses and disclosures. A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and

(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) Standard: requirements for a covered entity with multiple covered functions.

AMC/HIPAA Workgroup

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

§ 164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations.

(a) Standard: consent requirement. (1) Except as provided in paragraph (a)(2) or (a)(3) of this section, a covered health care provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.

(2) A covered health care provider may, without consent, use or disclose protected health information to carry out treatment, payment, or health care operations, if:

(i) The covered health care provider has an indirect treatment relationship with the individual; or

(ii) The covered health care provider created or received the protected health information in the course of providing health care to an individual who is an inmate.

AMC/HIPAA Workgroup

(3)(i) A covered health care provider may, without prior consent, use or disclose protected health information created or received under paragraph (a)(3)(i)(A)-(C) of this section to carry out treatment, payment, or health care operations:

(A) In emergency treatment situations, if the covered health care provider attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment;

(B) If the covered health care provider is required by law to treat the individual, and the covered health care provider attempts to obtain such consent but is unable to obtain such consent; or

(C) If a covered health care provider attempts to obtain such consent from the individual but is unable to obtain such consent due to substantial barriers to communicating with the individual, and the covered health care provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.

(ii) A covered health care provider that fails to obtain such consent in accordance with paragraph (a)(3)(i) of this section must document its attempt to obtain consent and the reason why consent was not obtained.

(4) If a covered entity is not required to obtain consent by paragraph (a)(1) of this section, it may obtain an individual's consent for the covered entity's own use or disclosure of protected health information to carry out treatment, payment, or health care operations, provided that such consent meets the requirements of this section.

AMC/HIPAA Workgroup

(5) Except as provided in paragraph (f)(1) of this section, a consent obtained by a covered entity under this section is not effective to permit another covered entity to use or disclose protected health information.

(b) Implementation specifications: general requirements. (1) A covered health care provider may condition treatment on the provision by the individual of a consent under this section.

(2) A health plan may condition enrollment in the health plan on the provision by the individual of a consent under this section sought in conjunction with such enrollment.

(3) A consent under this section may not be combined in a single document with the notice required by § 164.520.

(4)(i) A consent for use or disclosure may be combined with other types of written legal permission from the individual (e.g., an informed consent for treatment or a consent to assignment of benefits), if the consent under this section:

(A) Is visually and organizationally separate from such other written legal permission; and

(B) Is separately signed by the individual and dated.

(ii) A consent for use or disclosure may be combined with a research authorization under § 164.508(f).

(5) An individual may revoke a consent under this section at any time, except to the extent that the covered entity has taken action in reliance thereon. Such revocation must be in writing.

AMC/HIPAA Workgroup

(6) A covered entity must document and retain any signed consent under this section as required by § 164.530(j).

(c) Implementation specifications: content requirements. A consent under this section must be in plain language and:

(1) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment, or health care operations;

(2) Refer the individual to the notice required by § 164.520 for a more complete description of such uses and disclosures and state that the individual has the right to review the notice prior to signing the consent;

(3) If the covered entity has reserved the right to change its privacy practices that are described in the notice in accordance with § 164.520(b)(1)(v)(C), state that the terms of its notice may change and describe how the individual may obtain a revised notice;

(4) State that:

(i) The individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment, or health care operations;

(ii) The covered entity is not required to agree to requested restrictions; and

(iii) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;

(5) State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and

(6) Be signed by the individual and dated.

AMC/HIPAA Workgroup

(d) Implementation specifications: defective consents. There is no consent under this section, if the document submitted has any of the following defects:

(1) The consent lacks an element required by paragraph (c) of this section, as applicable; or

(2) The consent has been revoked in accordance with paragraph (b)(5) of this section.

(e) Standard: resolving conflicting consents and authorizations. (1) If a covered entity has obtained a consent under this section and receives any other authorization or written legal permission from the individual for a disclosure of protected health information to carry out treatment, payment, or health care operations, the covered entity may disclose such protected health information only in accordance with the more restrictive consent, authorization, or other written legal permission from the individual.

(2) A covered entity may attempt to resolve a conflict between a consent and an authorization or other written legal permission from the individual described in paragraph (e)(1) of this section by:

(i) Obtaining a new consent from the individual under this section for the disclosure to carry out treatment, payment, or health care operations; or

(ii) Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered entity must document the individual's preference and may only disclose protected health information in accordance with the individual's preference.

AMC/HIPAA Workgroup

(f)(1) Standard: joint consents. Covered entities that participate in an organized health care arrangement and that have a joint notice under § 164.520(d) may comply with this section by a joint consent.

(2) Implementation specifications: requirements for joint consents. (i) A joint consent must:

(A) Include the name or other specific identification of the covered entities, or classes of covered entities, to which the joint consent applies; and

(B) Meet the requirements of this section, except that the statements required by this section may be altered to reflect the fact that the consent covers more than one covered entity.

(ii) If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as practicable.

§164.508 Uses and disclosures for which an authorization is required.

(a) Standard: authorizations for uses and disclosures. (1) Authorization required: general rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) Authorization required: psychotherapy notes. Notwithstanding any other provision of this subpart, other than transition provisions provided for in § 164.532, a

AMC/HIPAA Workgroup

covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations, consistent with consent requirements in § 164.506:

(A) Use by originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(b) Implementation specifications: general requirements. (1) Valid authorizations.

(i) A valid authorization is a document that contains the elements listed in paragraph (c) and, as applicable, paragraph (d), (e), or (f) of this section.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not be inconsistent with the elements required by this section.

(2) Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects:

AMC/HIPAA Workgroup

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c), (d), (e), or (f) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization lacks an element required by paragraph (c), (d), (e), or (f) of this section, if applicable;

(v) The authorization violates paragraph (b)(3) of this section, if applicable;

(vi) Any material information in the authorization is known by the covered entity to be false.

(3) Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information created for research that includes treatment of the individual may be combined as permitted by § 164.506(b)(4)(ii) or paragraph (f) of this section;

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of

AMC/HIPAA Workgroup

treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.

(4) Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization under paragraph (f) of this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section;

(iii) A health plan may condition payment of a claim for specified benefits on provision of an authorization under paragraph (e) of this section, if:

(A) The disclosure is necessary to determine payment of such claim; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iv) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on

AMC/HIPAA Workgroup

provision of an authorization for the disclosure of the protected health information to such third party.

(5) Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.

(6) Documentation. A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) Implementation specifications: core elements and requirements. (1) Core elements. A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

(iv) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

AMC/HIPAA Workgroup

(v) A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

(vi) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;

(vii) Signature of the individual and date; and

(viii) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

(2) Plain language requirement. The authorization must be written in plain language.

(d) Implementation specifications: authorizations requested by a covered entity for its own uses and disclosures. If an authorization is requested by a covered entity for its own use or disclosure of protected health information that it maintains, the covered entity must comply with the following requirements.

(1) Required elements. The authorization for the uses or disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:

(i) For any authorization to which the prohibition on conditioning in paragraph (b)(4) of this section applies, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;

(ii) A description of each purpose of the requested use or disclosure;

AMC/HIPAA Workgroup

(iii) A statement that the individual may:

(A) Inspect or copy the protected health information to be used or disclosed as provided in § 164.524; and

(B) Refuse to sign the authorization; and

(iv) If use or disclosure of the requested information will result in direct or indirect remuneration to the covered entity from a third party, a statement that such remuneration will result.

(2) Copy to the individual. A covered entity must provide the individual with a copy of the signed authorization.

(e) Implementation specifications: authorizations requested by a covered entity for disclosures by others. If an authorization is requested by a covered entity for another covered entity to disclose protected health information to the covered entity requesting the authorization to carry out treatment, payment, or health care operations, the covered entity requesting the authorization must comply with the following requirements.

(1) Required elements. The authorization for the disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:

(i) A description of each purpose of the requested disclosure;

(ii) Except for an authorization on which payment may be conditioned under paragraph (b)(4)(iii) of this section, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure; and

AMC/HIPAA Workgroup

(iii) A statement that the individual may refuse to sign the authorization.

(2) Copy to the individual. A covered entity must provide the individual with a copy of the signed authorization.

(f) Implementation specifications: authorizations for uses and disclosures of protected health information created for research that includes treatment of the individual.

(1) Required elements. Except as otherwise permitted by § 164.512(i), a covered entity that creates protected health information for the purpose, in whole or in part, of research that includes treatment of individuals must obtain an authorization for the use or disclosure of such information. Such authorization must:

(i) For uses and disclosures not otherwise permitted or required under this subpart, meet the requirements of paragraphs (c) and (d) of this section; and

(ii) Contain:

(A) A description of the extent to which such protected health information will be used or disclosed to carry out treatment, payment, or health care operations;

(B) A description of any protected health information that will not be used or disclosed for purposes permitted in accordance with §§ 164.510 and 164.512, provided that the covered entity may not include a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i); and

(C) If the covered entity has obtained or intends to obtain the individual's consent under § 164.506, or has provided or intends to provide the individual with a notice under § 164.520, the authorization must refer to that consent or notice, as applicable, and state that the statements made pursuant to this section are binding.

AMC/HIPAA Workgroup

(2) Optional procedure. An authorization under this paragraph may be in the same document as:

- (i) A consent to participate in the research;
- (ii) A consent to use or disclose protected health information to carry out treatment, payment, or health care operations under § 164.506; or
- (iii) A notice of privacy practices under § 164.520.

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

A covered entity may use or disclose protected health information without the written consent or authorization of the individual as described by §§ 164.506 and 164.508, respectively, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) Standard: use and disclosure for facility directories.

(1) Permitted uses and disclosure. Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

- (A) The individual's name;
- (B) The individual's location in the covered health care provider's facility;

AMC/HIPAA Workgroup

- (C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and
- (D) The individual's religious affiliation; and
- (ii) Disclose for directory purposes such information:
 - (A) To members of the clergy; or
 - (B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) Emergency circumstances. (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

- (A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

AMC/HIPAA Workgroup

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) Standard: uses and disclosures for involvement in the individual's care and notification purposes.

(1) Permitted uses and disclosures. (i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.

(2) Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

AMC/HIPAA Workgroup

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

(3) Limited uses and disclosures when the individual is not present. If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) Use and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines

AMC/HIPAA Workgroup

that the requirements do not interfere with the ability to respond to the emergency circumstances.

§ 164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written consent or authorization of the individual as described in §§ 164.506 and 164.508, respectively, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) Standard: uses and disclosures required by law. (1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) Standard: uses and disclosures for public health activities.

(1) Permitted disclosures. A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

AMC/HIPAA Workgroup

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration:

(A) To report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations if the disclosure is made to the person required or directed to report such information to the Food and Drug Administration;

(B) To track products if the disclosure is made to a person required or directed by the Food and Drug Administration to track the product;

(C) To enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals, or other problems); or

(D) To conduct post marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration;

AMC/HIPAA Workgroup

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides a health care to the individual at the request of the employer:

(1) To conduct an evaluation relating to medical surveillance of the workplace; or

(2) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance;

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(1) By giving a copy of the notice to the individual at the time the health care is provided; or

AMC/HIPAA Workgroup

(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(2) Permitted uses. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) Standard: disclosures about victims of abuse, neglect or domestic violence.

(1) Permitted disclosures. Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation

and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

AMC/HIPAA Workgroup

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) Informing the individual. A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(d) Standard: uses and disclosures for health oversight activities.

(1) Permitted disclosures. A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

AMC/HIPAA Workgroup

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) Exception to health oversight activities. For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) Joint activities or investigations. Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

AMC/HIPAA Workgroup

(4) Permitted uses. If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

(e) Standard: disclosures for judicial and administrative proceedings.

(1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the

AMC/HIPAA Workgroup

covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(1) No objections were filed; or

(2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

AMC/HIPAA Workgroup

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a *qualified protective order* means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) Other uses and disclosures under this section. The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

AMC/HIPAA Workgroup

(f) Standard: disclosures for law enforcement purposes. A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) Permitted disclosures: pursuant to process and as otherwise required by law. A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(3) De-identified information could not reasonably be used.

AMC/HIPAA Workgroup

(2) Permitted disclosures: limited information for identification and location purposes. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) Permitted disclosure: victims of a crime. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose

AMC/HIPAA Workgroup

protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(ii) The individual agrees to the disclosure; or

(iii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) Permitted disclosure: decedents. A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) Permitted disclosure: crime on premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

AMC/HIPAA Workgroup

(6) Permitted disclosure: reporting crime in emergencies. (i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

- (A) The commission and nature of a crime;
- (B) The location of such crime or of the victim(s) of such crime; and
- (C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) Standard: uses and disclosures about decedents. (1) Coroners and medical examiners. A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) Funeral directors. A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors carry out their duties, the

AMC/HIPAA Workgroup

covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes. A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) Standard: uses and disclosures for research purposes. (1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

AMC/HIPAA Workgroup

(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) Research on decedent's information. The covered entity obtains from the researcher:

(A) Representation that the use or disclosure is sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

AMC/HIPAA Workgroup

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) Identification and date of action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than minimal risk to the individuals;

(B) The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;

(C) The research could not practicably be conducted without the alteration or waiver;

(D) The research could not practicably be conducted without access to and use of the protected health information;

(E) The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;

AMC/HIPAA Workgroup

(F) There is an adequate plan to protect the identifiers from improper use and disclosure;

(G) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

(H) There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.

(iii) Protected health information needed. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(D) of this section;

(iv) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28

AMC/HIPAA Workgroup

CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) Required signature. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) Standard: uses and disclosures to avert a serious threat to health or safety. (1) Permitted disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

AMC/HIPAA Workgroup

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) Use or disclosure not permitted. A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) Limit on information that may be disclosed. A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in

AMC/HIPAA Workgroup

paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) Presumption of good faith belief. A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) Standard: uses and disclosures for specialized government functions. (1) Military and veterans activities. (i) Armed Forces personnel. A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the **Federal Register** the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's

AMC/HIPAA Workgroup

eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) Veterans. A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) Foreign military personnel. A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the **Federal Register** pursuant to paragraph (k)(1)(i) of this section.

(2) National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333).

(3) Protective services for the President and others. A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

AMC/HIPAA Workgroup

(4) Medical suitability determinations. A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;

(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act;
or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) Correctional institutions and other law enforcement custodial situations. (i) Permitted disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

AMC/HIPAA Workgroup

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; and

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) Permitted uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) No application after release. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) Covered entities that are government programs providing public benefits. (i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a

AMC/HIPAA Workgroup

government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(1) Standard: disclosures for workers' compensation. A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(a) Standard: de-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

AMC/HIPAA Workgroup

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

AMC/HIPAA Workgroup

- (E) Fax numbers;
 - (F) Electronic mail addresses;
 - (G) Social security numbers;
 - (H) Medical record numbers;
 - (I) Health plan beneficiary numbers;
 - (J) Account numbers;
 - (K) Certificate/license numbers;
 - (L) Vehicle identifiers and serial numbers, including license plate numbers;
 - (M) Device identifiers and serial numbers;
 - (N) Web Universal Resource Locators (URLs);
 - (O) Internet Protocol (IP) address numbers;
 - (P) Biometric identifiers, including finger and voice prints;
 - (Q) Full face photographic images and any comparable images; and
 - (R) Any other unique identifying number, characteristic, or code; and
- (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

AMC/HIPAA Workgroup

(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) Standard: minimum necessary requirements. A covered entity must reasonably ensure that the standards, requirements, and implementation specifications of § 164.502(b) and this section relating to a request for or the use and disclosure of the minimum necessary protected health information are met.

(2) Implementation specifications: minimum necessary uses of protected health information. (i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) Implementation specification: minimum necessary disclosures of protected health information. (i) For any type of disclosure that it makes on a routine and recurring

AMC/HIPAA Workgroup

basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

AMC/HIPAA Workgroup

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) Implementation specifications: minimum necessary requests for protected health information. (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must review the request on an individual basis to determine that the protected health information sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

(5) Implementation specification: other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) Standard: uses and disclosures of protected health information for marketing. A covered entity may not use or disclose protected health information for

AMC/HIPAA Workgroup

marketing without an authorization that meets the applicable requirements of § 164.508, except as provided for by paragraph (e)(2) of this section.

(2) Implementation specifications: requirements relating to marketing. (i) A covered entity is not required to obtain an authorization under § 164.508 when it uses or discloses protected health information to make a marketing communication to an individual that:

(A) Occurs in a face-to-face encounter with the individual;

(B) Concerns products or services of nominal value; or

(C) Concerns the health-related products and services of the covered entity or of a third party and the communication meets the applicable conditions in paragraph (e)(3) of this section.

(ii) A covered entity may disclose protected health information for purposes of such communications only to a business associate that assists the covered entity with such communications.

(3) Implementation specifications: requirements for certain marketing communications. For a marketing communication to qualify under paragraph (e)(2)(i) of this section, the following conditions must be met:

(i) The communication must:

(A) Identify the covered entity as the party making the communication;

(B) If the covered entity has received or will receive direct or indirect remuneration for making the communication, prominently state that fact; and

AMC/HIPAA Workgroup

(C) Except when the communication is contained in a newsletter or similar type of general communication device that the covered entity distributes to a broad cross-section of patients, enrollees, or other broad groups of individuals, contain instructions describing how the individual may opt out of receiving future such communications.

(ii) If the covered entity uses or discloses protected health information to target the communication to individuals based on their health status or condition:

(A) The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and

(B) The communication must explain why the individual has been targeted and how the product or service relates to the health of the individual.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications, under paragraph (e)(3)(i)(C) of this section, are not sent such communications.

(f)(1) Standard: uses and disclosures for fundraising. A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual; and

(ii) Dates of health care provided to an individual.

(2) Implementation specifications: fundraising requirements. (i) The covered entity may not use or disclose protected health information for fundraising purposes as

AMC/HIPAA Workgroup

otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice;

(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

(g) Standard: uses and disclosures for underwriting and related purposes. If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.

(h)(1) Standard: verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such

AMC/HIPAA Workgroup

documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) Implementation specifications: verification. (i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

AMC/HIPAA Workgroup

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

§ 164.520 Notice of privacy practices for protected health information.

(a) Standard: notice of privacy practices. (1) Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of

AMC/HIPAA Workgroup

the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) Exception for group health plans. (i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected

AMC/HIPAA Workgroup

health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) Exception for inmates. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) Implementation specifications: content of notice.

(1) Required elements. The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) Header. The notice must contain the following statement as a header or otherwise prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”

(ii) Uses and disclosures. The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual’s written consent or authorization.

AMC/HIPAA Workgroup

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by § 164.508(b)(5).

(iii) Separate statements for certain uses or disclosures. If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:

(A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;

(B) The covered entity may contact the individual to raise funds for the covered entity; or

(C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

AMC/HIPAA Workgroup

(iv) Individual rights. The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) Covered entity's duties. The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

AMC/HIPAA Workgroup

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) Complaints. The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) Contact. The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) Effective date. The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) Optional elements. (i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

AMC/HIPAA Workgroup

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) Revisions to the notice. The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) Implementation specifications: provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(4) of this section, as applicable.

(1) Specific requirements for health plans. (i) A health plan must provide notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees;
and

(C) Within 60 days of a material revision to the notice, to individuals then covered by the plan.

AMC/HIPAA Workgroup

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(2) Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider;

(ii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

AMC/HIPAA Workgroup

(iii) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(ii) of this section, if applicable.

(3) Specific requirements for electronic notice. (i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) Implementation specifications: joint notice by separate covered entities. Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

AMC/HIPAA Workgroup

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

AMC/HIPAA Workgroup

(e) Implementation specifications: documentation. A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity as required by § 164.530(j).

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) Standard: right of an individual to request restriction of uses and disclosures. (i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) A covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

AMC/HIPAA Workgroup

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(i), 164.510(a) or 164.512.

(2) Implementation specifications: terminating a restriction. A covered entity may terminate its agreement to a restriction, if :

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

(3) Implementation specification: documentation. A covered entity that agrees to a restriction must document the restriction in accordance with § 164.530(j).

(b)(1) Standard: confidential communications requirements. (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual,

AMC/HIPAA Workgroup

(2) Implementation specifications: conditions on providing confidential communications.

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

§ 164.524 Access of individuals to protected health information.

(a) Standard: access to protected health information. (1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

AMC/HIPAA Workgroup

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) Unreviewable grounds for denial. A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the

AMC/HIPAA Workgroup

individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional

AMC/HIPAA Workgroup

judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) Review of a denial of access. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) Implementation specifications: requests for access and timely action.

(1) Individual's request for access. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) Timely action by the covered entity. (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

AMC/HIPAA Workgroup

(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.

(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) Implementation specifications: provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Providing the access requested. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than

AMC/HIPAA Workgroup

one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) Form of access requested. (i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

(ii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) Time and manner of access. The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

AMC/HIPAA Workgroup

(4) Fees. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;

(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

(d) Implementation specifications: denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) Denial. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

AMC/HIPAA Workgroup

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) Other responsibility. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) Review of denial requested. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

AMC/HIPAA Workgroup

(e) Implementation specification: documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):

- (1) The designated record sets that are subject to access by individuals; and
- (2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§ 164.526 Amendment of protected health information.

(a) Standard: right to amend.

(1) Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) Denial of amendment. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) Implementation specifications: requests for amendment and timely action.

(1) Individual's request for amendment. The covered entity must permit an individual to request that the covered entity amend the protected health information

AMC/HIPAA Workgroup

maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) Timely action by the covered entity. (i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) Implementation specifications: accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

AMC/HIPAA Workgroup

(1) Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) Implementation specifications: denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

AMC/HIPAA Workgroup

(1) Denial. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(2) Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the

AMC/HIPAA Workgroup

covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) Recordkeeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) Future disclosures. (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity

AMC/HIPAA Workgroup

may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) Implementation specification: actions on notices of amendment. A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) Implementation specification: documentation. A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.

(a) Standard: right to an accounting of disclosures of protected health information.

(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in § 164.502;

(ii) To individuals of protected health information about them as provided in § 164.502;

(iii) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;

(iv) For national security or intelligence purposes as provided in § 164.512(k)(2);

AMC/HIPAA Workgroup

(v) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5); or

(vi) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) Implementation specifications: content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements.

AMC/HIPAA Workgroup

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) The accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:

(A) A copy of the individual's written authorization pursuant to § 164.508; or

(B) A copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, or pursuant to a single authorization under § 164.508, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

AMC/HIPAA Workgroup

- (ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and
 - (iii) The date of the last such disclosure during the accounting period.
- (c) Implementation specifications: provision of the accounting.
- (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.
 - (i) The covered entity must provide the individual with the accounting requested;or
 - (ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:
 - (A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and
 - (B) The covered entity may have only one such extension of time for action on a request for an accounting.
 - (2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

AMC/HIPAA Workgroup

(d) Implementation specification: documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

§ 164.530 Administrative requirements.

(a)(1) Standard: personnel designations. (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) Implementation specification: personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) Standard: training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.

AMC/HIPAA Workgroup

(2) Implementation specifications: training. (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) Implementation specification: safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(d)(1) Standard: complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and

AMC/HIPAA Workgroup

procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

(2) Implementation specification: documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) Standard: sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) Implementation specification: documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) Standard: mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) Standard: refraining from intimidating or retaliatory acts. A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

AMC/HIPAA Workgroup

(1) Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;

(2) Individuals and others. Any individual or other person for:

(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;

(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(h) Standard: waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) Standard: policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to

AMC/HIPAA Workgroup

permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) Standard: changes to policies or procedures. (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) Implementation specification: changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

AMC/HIPAA Workgroup

(4) Implementation specifications: changes to privacy practices stated in the notice. (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation the requirements in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

AMC/HIPAA Workgroup

(5) Implementation specification: changes to other policies or procedures. A

covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) Standard: documentation. A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(2) Implementation specification: retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) Standard: group health plans. (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

AMC/HIPAA Workgroup

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

§ 164.532 Transition provisions.

(a) Standard: effect of prior consents and authorizations. Notwithstanding other sections of this subpart, a covered entity may continue to use or disclose protected health information pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information that does not comply with §§ 164.506 or 164.508 of this subpart consistent with paragraph (b) of this section.

(b) Implementation specification: requirements for retaining effectiveness of prior consents and authorizations. Notwithstanding other sections of this subpart, the following provisions apply to use or disclosure by a covered entity of protected health information pursuant to a consent, authorization, or other express legal permission

AMC/HIPAA Workgroup

obtained from an individual permitting the use or disclosure of protected health information, if the consent, authorization, or other express legal permission was obtained from an individual before the applicable compliance date of this subpart and does not comply with §§ 164.506 or 164.508 of this subpart.

(1) If the consent, authorization, or other express legal permission obtained from an individual permits a use or disclosure for purposes of carrying out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission obtained from an individual applies, use or disclose such information for purposes of carrying out treatment, payment, or health care operations, provided that:

(i) The covered entity does may not make any use or disclosure that is expressly excluded from the a consent, authorization, or other express legal permission obtained from an individual; and

(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(2) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for a purpose other than to carry out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal

AMC/HIPAA Workgroup

permission obtained from an individual applies, make such use or disclosure, provided that:

(i) The covered entity does not make any use or disclosure that is expressly excluded from the consent, authorization, or other express legal permission obtained from an individual; and

(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(3) In the case of a consent, authorization, or other express legal permission obtained from an individual that identifies a specific research project that includes treatment of individuals:

(i) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for purposes of the project, the covered entity may, with respect to protected health information that it created or received either before or after the applicable compliance date of this subpart and to which the consent or authorization applies, make such use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(ii) If the consent, authorization, or other express legal permission obtained from an individual is a general consent to participate in the project, and a covered entity is conducting or participating in the research, such covered entity may, with respect to protected health information that it created or received as part of the project before or after the applicable compliance date of this subpart, make a use or disclosure for purposes

AMC/HIPAA Workgroup

of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

AMC/HIPAA Workgroup

(4) If, after the applicable compliance date of this subpart, a covered entity agrees to a restriction requested by an individual under § 164.522(a), a subsequent use or disclosure of protected health information that is subject to the restriction based on a consent, authorization, or other express legal permission obtained from an individual as given effect by paragraph (b) of this section, must comply with such restriction.

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) Health care providers. A covered health care provider must comply with the applicable requirements of this subpart no later than [OFR - insert date 24 months after the effective date of the final rule in the **Federal Register**].

(b) Health plans. A health plan must comply with the applicable requirements of this subpart no later than the following date, as applicable:

(1) Health plans other than small health plans – [OFR - insert date 24 months after the effective date of the final rule in the **Federal Register**].

(2) Small health plans – [OFR - insert date 36 months after the effective date of the final rule in the **Federal Register**].

(c) Health care clearinghouses. A health care clearinghouse must comply with the applicable requirements of this subpart no later than [OFR - insert date 24 months after the effective date of the final rule in the **Federal Register**].