

---

**WEDI - Strategic National Implementation Process  
(SNIP)**

# **Privacy Policies and Procedures: A Resource Document**



**SNIP**

**Privacy Policies & Procedures:  
A Resource Document  
Discussion DRAFT Version 2.0**

***Workgroup for Electronic Data Interchange***

*12020 Sunrise Valley DR., Suite 100, Reston, VA. 20191*

*(t) 703-391-2716 / (f) 703-391-2759*

© 2002 Workgroup for Electronic Data Interchange, All Rights Reserved

# Contents

<b>Contents .....</b>	<b>i</b>
<b>Policies &amp; Procedures Workgroup.....</b>	<b>3</b>
Background .....	3
Disclaimer .....	3
Definition .....	3
Objectives.....	4
Implementation Considerations and Issues .....	5
Risk Considerations.....	6
<b>General Topics .....</b>	<b>8</b>
Organizational Requirements - An Overview .....	9
Organizational Requirements - Affiliated covered entity .....	13
Organizational Requirements: Business Associates.....	15
Organizational Requirements - Group Health Plans .....	20
Organizational Requirements - Hybrid Entities .....	24
Organizational Requirements – Organized Health Care Arrangements.....	27
Preemption of State Law .....	30
<b>Administrative Requirements.....</b>	<b>32</b>
Administrative Requirements - Changes in Law.....	33
Administrative Requirements - Complaint Process .....	35
Administrative Requirements - Designation of Privacy Official and Contact Person.....	37
Administrative Requirements - Documentation.....	39
Administrative Requirements - Mitigation.....	42
Administrative Requirements - Sanctions By Covered Entities Against Members of Its Workforce .....	43
Administrative Requirements - Safeguards.....	45
Administrative Requirements - Training For Staff .....	47
Administrative Requirements – Whistleblowers and Workforce Crime Victims .....	49
<b>Individual Rights.....</b>	<b>51</b>
Individual’s Rights - Accounting of Disclosures .....	52
Individual’s Rights - to Inspect and Copy .....	56
Individual Rights - Notice of Privacy Practices .....	60

Individual's Rights - Request Amendment .....	67
Individual's Rights - Request Confidential Communications.....	71
Individual's Rights - Request Restriction of Uses and Disclosures .....	73
<b>Uses and Disclosures.....</b>	<b>75</b>
Use and Disclosures - Authorizations .....	76
Use and Disclosure – Communications with Brokers and Agents.....	80
Use and Disclosure – Deceased Individuals.....	82
Use and Disclosure - De-identification of Protected Health Information .....	84
Use and Disclosure - Emergency Situations .....	88
Use and Disclosure – To Employer/Plan Sponsor .....	90
Use and Disclosure - Marketing and Fundraising .....	93
Uses and Disclosure – Not Requiring an Authorization or Opportunity for the Individual to Agree or Object .....	96
Use and Disclosure - Minimum Necessary .....	100
Uses and Disclosures – Permitted Under the Privacy Rule.....	104
Use and Disclosure - Personal Representatives.....	108
Use and Disclosure - Required by Law.....	111
Uses and Disclosures - Requiring an Opportunity for the Individual to Agree or to Object.....	115
Use and Disclosure - Research Activities .....	120
Use and Disclosure - Underwriting and related purposes .....	124
Use and Disclosure - Verification of Identity and Authority of Entities Requesting PHI .....	126
Use & Disclosure - Victims of Abuse, Neglect, Domestic Violence, and Crime.....	130
Appendix A: Privacy and Security Terminology .....	134
Appendix B: Resources.....	141
<b>APPENDIX C: Use and Disclosures - Consent .....</b>	<b>143</b>
<b>Acknowledgements .....</b>	<b>147</b>
<b>Privacy Policies &amp; Procedures Checklist.....</b>	<b>149</b>

# Policies & Procedures Workgroup

## Background

Both the final HIPAA Privacy Rule and the proposed HIPAA Security Rule require that a covered entity develop policies and procedures to implement the Rules' requirements. While it is not the intent of the WEDI SNIP Privacy and Security workgroup to provide sample policies and procedures, the workgroup established the Policies and Procedures sub-workgroup to develop two white papers that will serve as resources to provide substantial assistance in developing policies and procedures for the HIPAA Privacy and Security Rules. The Security and Privacy workgroup believes that these white papers will provide useful guides on which policies and procedures a covered entity needs to develop for each rule as well as background information necessary for each organization to develop appropriate policies and procedures. This white paper is the resource document for the final HIPAA Privacy Rule, as modified on August 14, 2002 (the "Final HIPAA Privacy Rule as Modified").

## Disclaimer

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual Security and Privacy workgroup members. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by WEDI or individual workgroup members. The listing of an organization does not imply any sort of endorsement and WEDI takes no responsibility for the products, tools, and Internet sites listed.

## Definition

In section 164.530(i), Administrative Requirements, the Final HIPAA Privacy Rule as Modified states the requirement to develop policies and procedures:

*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.*

Having developed policies and procedures, a covered entity must change its policies and procedures when "necessary and appropriate" to comply with changes in the law and/or changes in the entity's privacy practices. A covered entity must document all policies and procedures and update its documentation whenever it makes changes to its privacy practices, policies and procedures.

The documentation of policies and procedures may be either in written or electronic form. A covered entity must retain this documentation for six (6) years from the date it was created or was last in effect, whichever is later.

A special exception to these administrative requirements exists for any **group health plan** that meets the following criteria:

- Provides health benefits solely through a contract with an insurance issuer or an HMO
- Does not create or receive protected health information except for summary information or basic enrollment information

See Organizational Requirements: Group Health Plans.

## Objectives

The objective of the Policies and Procedures subgroup in this white paper is to provide guidance to covered entities regarding those parts of the Final HIPAA Privacy Rule as Modified that require development of policies and procedures. Please note that this white paper is based on the Final HIPAA Privacy Rule published in the Federal Register on December 28, 2000 (65 Fed. Reg. 82,462), as modified in the August 14, 2002 Federal Register (67 Fed. Reg. 51,181). In this white paper, we refer to this as the Final HIPAA Privacy Rule as Modified. For the reader's convenience, this white paper will reference an integrated version of the Final HIPAA Privacy Rule as Modified published at <http://www.hhs.gov/ocr/combinedregtext.pdf>. Where appropriate, we also used the first Privacy Guidance issued by the U.S. Department of Health and Human Services (HHS) on July 3, 2001, as a source of information. The Department of Health and Human Services has stated that further Guidance may be forthcoming. Consequently, this white paper is subject to revision. A revision date at the beginning of each topic indicates the date that particular topic was last revised. Any modifications to the rule or any additional Guidance issued after that date were not used as a resource for the topic.

The Policies and Procedures subgroup set the following goals for this white paper:

- Identify areas in the Final HIPAA Privacy Rule as Modified specifically requiring development of policies and procedures.
- Cite specific sections of Final HIPAA Privacy as Modified and the various HHS Preambles that reference the standard and the requirements for policies and procedures. In this white paper, we will refer to the HHS Preamble published in the December 28, 2000, Federal Register as the "Preamble to the Final Rule" and to the HHS Preamble published in the August 14, 2002, Federal Register as the "Preamble to the Modifications." Where there are numerous references from the Preambles relating to a topic, we have cited those references that are substantive and provide clarification to the text of the Final HIPAA Privacy Rule as Modified. There may be additional references to a topic in one of the Preambles that are not included because the group judged them to be less germane. At a future date, the workgroup may be able to provide an index that would include all references to a topic.
- Provide both an explanation of the general requirements of the standard and any specific requirements regarding the policies and procedures needed to implement the standard.
- Create a checklist of areas requiring development of policies and procedures.
- Include a glossary of Privacy terminology.

- Assemble a list of websites and other resources to provide additional information regarding policies and procedures.

## Implementation Considerations and Issues

Each covered entity is required to establish policies and procedures to ensure compliance with the Final HIPAA Privacy Rule as Modified. Individual differences, such as size and technological sophistication, will influence the specific policies and procedures that a covered entity develops. Because the Final HIPAA Privacy Rule as Modified is intended to be flexible and scalable, larger, more technologically sophisticated covered entities are required to implement more extensive and more stringent privacy policies and procedures.

The Final HIPAA Privacy Rule as Modified's administrative requirements are similar to the compliance program requirements established in Chapter 8 of the Federal Sentencing Guidelines (<http://www.ussc.gov/2001guid/TABCON01.htm>) and the HHS OIG's Compliance Program Guidance (<http://oig.hhs.gov/fraud/complianceguidance.html#1>). If your organization has developed either of these programs, that experience will be valuable in developing the HIPAA mandated policies and procedures. Please note that a compliance program which takes the Federal Sentencing Guidelines into account may be helpful in avoiding or mitigating criminal penalties for wrongful disclosure of individually identifiable health information under HIPAA §1177.

Three critical steps that organizations generally must take before drafting the policies and procedures are:

1. Determine how the Final HIPAA Privacy Rule as Modified's Organizational Requirements (§164.504) apply to your organization. Once you have determined that your organization is a covered entity that is obligated to prepare policies and procedures, it is essential to analyze, for example, whether due to the existence of non-covered functions, your organization should become a "hybrid entity" or whether due to your organization's relationship to other covered entities, it should be an "Affiliated covered entity" or part of an "Organized Health Care Arrangement." The application of the Organizational Requirements can have a significant impact on the drafting of the policies and procedures.
2. "Inventory" your organization's protected health information ("PHI"). The Final HIPAA Privacy Rule as Modified's objective is to safeguard PHI – in all of its forms, written, electronic, and oral -- by limiting internal uses and external disclosures to permissible purposes – principally Treatment, Payment, and Health Care Operations ("TPO"). To implement the Final HIPAA Privacy Rule as Modified, you need to document where your organization's PHI is stored, the sources of the PHI, and the internal users, external users, and requesters of the PHI and why each user accesses the PHI. It is helpful to describe this process as an inventory, and like any inventory it must be kept current.
3. Assemble and assess your existing privacy and security policies and practices related to PHI. Many organizations will have written policy and procedural documents that are relevant to PHI safeguards, but these probably do not adequately address all requirements found in the Final HIPAA Privacy Rule as Modified. It may also be the case that there are no published policies on significant issues, and that actual practices deviate from published policies or those appropriate under the Final HIPAA Privacy Rule as Modified. If possible, existing documentation may be revised to support the new requirements. Starting from existing documentation will also help in educating personnel who have been trained and have worked

under a set of policies and procedures or relied upon practices that will be changing to accommodate the Final HIPAA Privacy Rule as Modified.


To facilitate the actual drafting of policies and procedures, we have prepared, as Appendix D- to this white paper, a checklist that ties back to the sections of this document. However, the policies and procedures listed in the checklist reflect the workgroup's best effort to detail the areas requiring development of policies and procedures. It should **not** be considered to be a complete listing of all possible policies and procedures. Nor is it intended to be a comprehensive listing of "best practices" for privacy and security. Rather, the group specifically limited itself to those topics that are clearly addressed within the Final HIPAA Privacy Rule as Modified.

Covered entities should also consider the need to publish notices and forms, such as authorizations, in "plain language," including those languages used by any substantial non-English speaking group in the covered entity's market. "Plain language" is explicitly required for the notice of privacy practices under §164.520(b)(1) of the Final HIPAA Privacy Rule as Modified, and it would be prudent to ensure that related documentation, such as authorizations, used with the covered entity's patients or members is consistent with this standard. In some areas it may also be desirable to publish some employee policies in other languages for any substantial portion of the workforce that may have difficulty with English. While not required by the Final HIPAA Privacy Rule as Modified, this may be a prudent tactic to ensure appropriate awareness on the part of such employees.

Finally, once your organization has drafted its policies and procedures, do not overlook the necessity to create a process for keeping those policies and procedures current.

## Risk Considerations

A covered entity's decisions regarding the scope of its policies and procedures can be influenced by physical factors such as its size and by business factors such as acceptable levels of risk. Even the smallest entity must implement appropriate policies and procedures required to protect the health information in its care. However, larger and more sophisticated entities will be expected to implement policies and procedures that reflect their size and complexity.

 **Critical: State Regulations:** With certain limited exceptions, a provision of the Final HIPAA Privacy Rule as Modified preempts state law if:

- That provision is more stringent than the state law, and
- It would be impossible for a covered entity to comply with both that provision and the state law and the Final HIPAA Privacy Rule as Modified; or
- The state law creates an obstacle to accomplishment of the goals of the Final HIPAA Privacy Rule as Modified.

Covered entities must be aware of state laws that are more stringent than the Final HIPAA Privacy Rule as Modified and generally must meet the higher standards in every instance. (This is being addressed by the Preemption workgroup.)

While all covered entities (except certain group health plans) must comply with the policies and procedures standards, covered entities with a history of HHS compliance issues related to other HHS-administered programs, such as Medicare, should be particularly careful to demonstrate compliance with the standards, as they are most likely to come under further HHS scrutiny. In addition, covered entities have to be sensitive to any particular needs and concerns of their

communities. To the extent possible, covered entities should meet the expectations of their patients or members.

# General Topics

# Organizational Requirements - An Overview

*Revision Date: 09/06/2002*

## Citations

Several sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address the organizational requirement standards and the policies and procedures required to implement the standards:

- §160.103(2)(i) Definitions – Business Associate, Covered entity, Group health plan, Health plan
- §164.501 Definitions – Covered functions
- §164.504(a) Definitions – Common control, Common ownership, Health care component, and Hybrid entity
- §164.504(b),(c) – Standard: Health care component/Hybrid entity
- §164.504(d) (1), (2), & (3) – Affiliated covered entities
- §164.504(e) – Standard: Requirements for Business associate contracts
- §164.504(f) – Standard: Requirements for group health plans
- §164.504(g) – Standard: Requirements for a covered entity with multiple covered functions
- §164.530(i) – Standard: Policies and Procedures
- §164.530(j) – Standard: Documentation
- Preamble to the Final Rule, pg. 82,502–03, 82,507-09, 82,637, and 82,645 – HHS Discussion of Organizational Requirements
- Preamble to the Modifications, pg. 53,203–08 – HHS Discussion of Organizational Requirements

## General Requirements

The Final HIPAA Privacy Rule as Modified applies to certain covered entities – health care providers who engage in one or more the HIPAA Standard Transactions, directly or indirectly, for example, through a billing service, health care clearinghouses, and health plans. The Final HIPAA Privacy Rule as Modified recognizes that these health care organizations are necessarily complex. A covered entity may perform many functions that are not covered functions under the Final HIPAA Privacy Rule as Modified, or may manage many types of services and products, including insurance products that are considered excepted benefits, such as workers compensation or life insurance, and not regulated by the Final HIPAA Privacy Rule as Modified. It is its covered functions that make a health plan, health care provider, or health care clearinghouse a covered entity.

In applying the Final HIPAA Privacy Rule as Modified, other non-covered functions may be impacted within the covered entity organization. At the same time, an entity that would not ordinarily qualify under the definition of a health plan, health care provider, or health care

clearinghouse may provide covered functions through its affiliation or contract with a covered entity. Additionally, the Final HIPAA Privacy Rule as Modified recognizes that legally distinct entities may share common administration and therefore may create a common compliance approach.

In order to accommodate these varied circumstances, the Final HIPAA Privacy Rule as Modified introduces the concepts of hybrid entities, business associates, affiliated covered entities, organized health care arrangements, and multiple covered functions. Before approaching organization-wide policies and procedures, it is important for a covered entity to determine if any of these concepts apply. A covered entity must review its corporate structure, its affiliates, its functions performed, and its delegated functions to determine how the Final HIPAA Privacy Rule as Modified must be applied to the whole entity - including any affiliates or business associates. Documentation of the designation of the organizational structure and affiliations is required. The choice of designation may affect such matters as organizational control and reporting relationships, which raise significant secondary issues potentially affecting tax status or liability for other parties. For this reason legal counsel must play a role in this process, and the choice of designation should ordinarily be subject to board or other appropriate governance-level oversight.

### **Hybrid Entity**

According to the definition in §164.504(a), a single legal entity that is a covered entity and whose business activities include both covered and non-covered functions may become a “hybrid entity” by designating its health care components. This designation must be documented.

Because the Final HIPAA Privacy Rule as Modified applies only to the health care components of a hybrid entity, there must be a separation, including applicable safeguards, of the information and responsibilities in each component of the entity (the covered health care component and the non-covered component) as if they were distinct legal entities.

The requirements of the hybrid entity are explored more thoroughly under the subtopic Privacy Policies and Procedures: Organizational Requirements – Hybrid Entities.

### **Business Associate**

A business associate is a person or entity who is not a member of the covered entity’s work force and who, on the covered entity’s behalf, performs or assists in the performance of a function or activity involving the use of individually identifiable health information. Section 164.504(e) of the Final HIPAA Privacy Rule as Modified describes an organizational requirement to establish a contract with these individuals or entities that perform delegated services.

The circumstances that create a business associate relationship and the requirements of the business associate contracts are explored more thoroughly under the subtopic Organizational Requirements: Business Associates.

### **Affiliated Covered Entities**

As outlined in §164.504(d), a covered entity comprised of legally separate covered entities that are affiliated may designate itself as a single covered entity for compliance purposes under the Final HIPAA Privacy Rule as Modified. The legally separate entities must be under common ownership or common control to be eligible for this designation. Common ownership is defined in §164.504(a) as an entity possessing an ownership or equity interest of five percent or more in another entity. Common control is defined in the same subsection as an entity having power, directly or indirectly, to influence or direct the actions or policies of another entity.

As described in §164.504(d)(2)(ii), once an organization decides to choose the designation of an affiliated covered entity, that entity must document the designation. The subsequent requirements of the affiliated covered entity are explored more thoroughly under the subtopic: Organizational Requirements – Affiliated Covered Entities.

### **Covered Entities with Multiple Covered Functions**

This designation applies to a single covered entity (or affiliated covered entities designated as a single covered entity) performing covered functions that qualify it as a covered entity under multiple entity types, i.e., health care provider, health care clearinghouse, health plan. This would apply to an integrated delivery network that is both a health plan and a provider of health care services or to a health plan that provides clearinghouse services to other health plans or providers. In these cases, the entity must comply with the standards as applicable to each component of its business. Furthermore, it must use and disclose the information pertaining to each component of its business only as would be allowed if they were separate entities. For example, if the health plan component receives and stores protected health information in the form of claims history on an individual, it could not make this information available to an affiliated hospital unless that hospital were the provider who rendered the services and then only to carry out treatment, payment and health care operations, unless an appropriate authorization were in place.

The policies, procedures and safeguards required to segregate multiple covered functions are similar to those required between the covered and non-covered functions of a hybrid entity. Similarly, the Final HIPAA Privacy Rule as Modified seeks to segregate the data available between the health plan component and the employer or plan sponsor component by laying out specific organizational requirements for group health plans.

### **Organized Health Care Arrangements**

This designation may be applied to integrated delivery systems and certain other relationships between or among covered entities, such as an individual practice association, to permit the participating covered entities to share protected health information for health care operations purposes and to utilize joint authorizations, notices of privacy practices, and business associate contracts.

### **Policies and Procedures**

Once an organization has determined whether the concepts of hybrid entity, business associate, affiliated covered entity, organized health care arrangement, or multiple covered functions apply, the affected entities should formally document this designation and consider the impact to policies and procedures enterprise-wide. There are many specific policy and procedural requirements of the hybrid entity, affiliated covered entity, or that entity performing multiple covered functions. These are discussed in the Final HIPAA Privacy Rule as Modified and will be explored further in later sections of this document.

In general, organizational policies and procedures for complex organizations such as these must include assurances of appropriate control mechanisms for these unique characteristics.

- Hybrid entities, affiliated covered entities, organized health care arrangements, and covered entities performing multiple covered functions and entities that delegate services to business associates must have a mechanism to ensure that all components of the organization are included in policy updates, training programs and compliance audits.

- Covered entities utilizing business associates must ensure that those responsible for deploying policy and maintaining contracts are aware of all business associate relationships, create or amend contracts with business associates as required by the Final HIPAA Privacy Rule as Modified, and have a mechanism to be notified of changes to those relationships.

Hybrid entities, group health plans and other covered entities performing multiple covered functions must have appropriate mechanisms to control the flow of data from one component of the organization to another. Furthermore, they must account for adequate separation when staff is shared between the components.

Each of these topics warrants further research in their application to your organization. In order to cover the subject matter that applies to these complex organizations more thoroughly, the following additional papers are included in this Policies & Procedures white paper:

Organizational Requirements - Hybrid Entities; Organizational Requirements - Affiliated Covered Entities; Organizational Requirements - Group Health Plans; and Organizational Requirements - Business Associates, and Organizational Requirements – Organized Health Care Arrangements.

# Organizational Requirements - Affiliated covered entity

*Revision Date: 09/06/2002*

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss the organizational requirements for an affiliated covered entity.

- §164.501 – Definitions: Covered functions
- §164.504(a) – Definitions: - Common control, common ownership, healthcare component
- §164.504 (b) – Standard: Health care component
- §164.504 (d)(1) – Standard: Requirements for designation of an affiliated covered entity
- §164.504 (d)(2) – Implementation specifications: Requirements for designation of an affiliated covered entity
- §164.504 (d)(3) – Implementation specifications: Safeguard requirements
- §164.504 (g) – Standard: Requirements for a covered entity with multiple covered functions
- §164.530 (i) – Standard: Policies and Procedures
- §164.530 (j) – Standard: Documentation
- Preamble to the Final Rule, pg. 82503 – Discussion of organizational requirements for affiliated covered entities
- Preamble to the Final Rule, pg. 82637 – Discussion of comments related to organizational requirements for affiliated covered entities

## General Requirements

The Final HIPAA Privacy Rule as Modified allows legally separate covered entities that are affiliated to designate themselves as a single covered entity – i.e., an affiliated covered entity – for compliance purposes. The benefit is that these entities may share common administration and thereby create a common approach to compliance with the rule.

As outlined in §164.504(d), to be eligible for the affiliated covered entity designation, the legally separate entities must be under common ownership or common control:

- Common ownership is defined in §164.504(a) as an entity possessing an ownership or equity interest of five percent or more in another entity.
- Common control is defined in §164.501(a) as an entity having power, directly or indirectly, to significantly influence or direct the actions or policies of another entity.

The affiliated covered entity designation can be applied to the health care component of a covered “hybrid entity.” A health care component is (1) the part of a covered entity that performs covered functions (i.e., those functions that make the covered entity a health plan, health care provider, or

health care clearinghouse) and (2) the part of a covered entity that performs activities that would make it a business associate of the part that performs covered functions if they were separate legal entities.

An affiliated covered entity must ensure that it is using and disclosing protected health information in accordance with the Final HIPAA Privacy Rule as Modified throughout the affiliated covered entity (§164.504 (d) (3)). Additionally, if the affiliated covered entity combines functions of a health plan, health care provider or health care clearinghouse, then:

- The covered entity must comply with the standards as applicable to each covered function of its business, and
- It must use and disclose the information of individuals who receive either the affiliated covered entity's health plan services or health care provider services, but not both, only as would be allowed for the appropriate function being performed. See Organizational Requirements: Multiple Covered Functions.

## **Policies and Procedures**

Once an organization has decided to elect affiliated covered entity status, it must document the designation and retain the documentation in written or electronic form for six (6) years from date of creation or date when it was last in effect, whichever is later (§164.504(d)(2)(ii)).

Suggestions for information to include in the documented designation:

- The covered entities deemed an affiliated covered entity.
- Specific health care components, if applicable, within a covered entity that are part of the affiliated covered entity.
- The criteria applied (common ownership, common control) to establish the affiliated covered entity under the Final HIPAA Privacy Rule as Modified.
- Policy statements that the affiliated covered entity will use and disclose protected health information in accordance with the Final HIPAA Privacy Rule as Modified. The documentation also should address issues such handling the joint BA contracting process, updating the joint notice of privacy practices, and addressing how to handle/communicate revocation of a joint authorization.
- Additional policy statements for affiliated entities with multiple covered functions ensuring that the applicable requirements are applied to the appropriate covered functions and that each component uses and discloses information as allowed as if the components were separate entities. Illustrative examples, applicable to the affiliated entity's business, would be helpful.

The covered entities participating in the affiliated covered entity arrangement may wish to provide each other with mutual indemnification in the event of a violation of the Final HIPAA Privacy Rule as Modified by one of them.

# Organizational Requirements: Business Associates

*Revised 09/06/2002*

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address requirements related to business associates. The term “business associate” is defined and the circumstances under which protected health information may be disclosed to or used by a business associate are prescribed in the following sections of 45 CFR Parts 160 and 164:

- §160.103 – Definitions - Business Associates, Workforce
- §164.502(e) – Uses and disclosures of protected health information: General rules – *Standard: Disclosures to business associates*
- §164.504(e) – Uses and disclosures: Organizational requirements -- *Standard: Business associate contracts*
- §164.532(e) – Transition Provisions – Effect of prior contracts or other arrangements with business associates
- Preamble to the Final Rule, pg. 82,475-76 – HHS Commentary on Definition of Business Associate
- Preamble to the Final Rule, pg. 82,480 – HHS Commentary on Definition of Workforce
- Preamble to the Final Rule, pg. 82,499 & 82,503-07 – HHS discussion of business associate standard
- Preamble to the Final Rule, pg. 82,640-48 – HHS discussion of public comments on proposed rule related to business associates
- Preamble to the Final Rule, pg. 82,579 – HHS discussion of public comments on proposed rule relating to workforce
- First Guidance on the Privacy Rule 07/06/01 – Business Associates
- Preamble to the Modifications, pg. 53,248–54 – HHS discussion of business associate provisions and transition rule
- Appendix to the Preamble to the Modifications, pg. 53,262-66 – Sample Business Associate Contract Provisions

## General Requirements

Section 160.103 of the Final HIPAA Privacy Rule as Modified defines a “Business Associate” as a person who acts in a capacity other than as a member of the workforce of a covered entity to perform or assist in the performance of a function or activity involving the use or disclosure of individually identifiable health information, or any other function or activity otherwise governed by the Final HIPAA Privacy Rule as Modified. Examples of activities or functions that may be performed by a business associate of a covered entity include:

- Claims processing or administration
- Utilization review
- Data analysis, processing or administration
- Billing
- Quality assurance
- Benefit management
- Billing
- Practice management
- Practice management
- Re-pricing

Business associates may also include persons who provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to covered entities if the business associate receives protected health information from the covered entity in the course of providing such services. A covered entity may be the business associate of another covered entity in certain circumstances.<sup>1</sup> As a resource, we have provided a Business Associate Decision Tree at the end of this topic.

A covered entity may have difficulty distinguishing between a business associate and a member of its workforce. The workforce consists of employees, volunteers, trainees, agents, and other persons under the direct control of the covered entity, regardless of whether they are paid by the covered entity. The distinction between a business associate and a member of the workforce is important because the definition of “business associate” (and therefore the requirement of a business associate contract) excludes members of the covered entity’s workforce. In addition, the obligations and potential liabilities of the covered entity and the person or entity in question differ depending on whether the person or entity is a business associate or a member of the workforce. For example, a covered entity is liable for violations of the HIPAA Administrative Simplification Rules by members of its workforce and is not generally liable for the actions of its business associates. Further, a business associate is not directly liable under the Final HIPAA Privacy Rule as Modified (except potentially under the criminal liability provisions of HIPAA §1177) but is liable to the covered entity for violations of its business associate contract.

Independent contractors, volunteers, and employees of a covered entity’s vendors or service providers may pose special classification problems for covered entities. The Preamble states that if the assigned workstations of persons under a service contract are on the covered entity’s premises, and those persons perform a substantial proportion of their activities at that location, the covered entity has the choice to treat them as either business associates or as part of the workforce. If the covered entity chooses to treat these persons as business associates, it must document its decision by having business associate contracts with these persons. If the covered entity does not have business associate contracts in place to cover such persons, the Preamble states that they are assumed to be members of the covered entity’s workforce. On the other hand,

---

<sup>1</sup> The Notice of Proposed Rulemaking issued on March 27, 2002, clarified HHS’s position that health care providers are not required to have business associate contracts in order to share protected health information for treatment purposes. Furthermore, according to HHS, discount payment arrangements between a health care provider and a health plan do not require business associate relationships. 67 Fed. Reg. 14788.

the Final HIPAA Privacy Rule as Modified is different for volunteers. If a volunteer works on the covered entity's premises, the covered entity may choose to treat the volunteer as a member of its workforce or as a business associate. However, covered entities do not have this choice for volunteers who perform their work off-site and who require PHI to perform their jobs. In this situation, the covered entity must have a business associate contract with the volunteer.

Before a covered entity may disclose protected health information to a business associate, "it must obtain satisfactory assurances that the business associate will appropriately safeguard the information." Section 164.502(e)(1). The business associate must provide these assurances by means of a written contract or other agreement that documents the permitted and required uses and disclosures of protected health information by the business associate. At a minimum, the business associate cannot use or disclose the information in any manner that would not be permissible for the covered entity under the Final HIPAA Privacy Rule as Modified.

The preferable contracting strategy is for the covered entity to specify those uses and disclosures which are permitted, because in most cases it would not be appropriate for the business associate to engage in many of the uses or disclosures that the covered entity is permitted to make. For example, a billing company, which is the business associate of a covered entity hospital, should not be permitted to use or disclose protected health information to the same extent that the hospital can. To avoid this result, the hospital should specify the billing company's authorized uses of protected health information in the business associate agreement.

Furthermore, the business associate must contractually agree that it will:

- Not use or further disclose the information other than as permitted under the contract or as required by law;
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided by its contract;
- Report to the covered entity any use or disclosure not provided for by its contract of which it becomes aware;
- Ensure that any agents or subcontractors to whom it provides protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information;
- Afford individuals access to their protected health information as required under Section 164.524;
- Make information available for amendment and incorporate amendments to it in accordance with Section 164.526;
- Make available the information to provide an accounting of disclosures in accordance with Section 164.528;
- Make its internal practices, books and records relating to the use and disclosures 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 the purposes of assessing the covered entity's compliance with the Final HIPAA Privacy Rule as Modified; and

At the 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.

The Final HIPAA Privacy Rule as Modified generally requires that a current business associate accept these contract provisions before the Final HIPAA Privacy Rule as Modified compliance date applicable to the covered entity. The Final HIPAA Privacy Rule as Modified allows covered

entities a transition period for modifying business associate contracts that are in effect on October 14, 2002. The covered entity and business associate may delay incorporating the business associate provisions in their contract beyond April 14, 2003, until the occasion otherwise arises to modify or renew the contract, provided, however, that in any event the business associate contract provisions must be incorporated no later than April 14, 2004. Business associate provisions must be incorporated into agreements that do qualify for the transition period, i.e., an agreement negotiated after October 14, 2002, no later than April 14, 2003.

## **Policies and Procedures**

### **Identification of Business Associates**

The first step in the policy and procedure development process is to identify business associates. In order to do so, covered entities will need to track the flow of protected health information from within their organizations to persons who are not part of their workforce. Covered entities also will need to develop processes for keeping this PHI tracking data current and for identifying additional business associates as new business relationships form.

Next the covered entity must evaluate whether each such disclosure is consistent with its permissible uses and disclosures policies, including the minimum necessary rule. If the disclosure is inappropriate under the Final HIPAA Privacy Rule as Modified, then the covered entity must halt the disclosure practice before the Rule's compliance date. If the continuing disclosure is appropriate, then the covered entity may use the Business Associate Decision Tree found on page 14 to evaluate whether or not this individual or entity which has access to your organization's protected health information is a business associate.

### **Business Associate Contracting**

With respect to those business associates, the covered entity must take the following steps:

- Develop standardized business associate contract language incorporating the required obligations discussed above. HHS published a Sample Business Associate Agreement in the August 14, 2002, Federal Register (67 Fed. Reg. 53,262).
- Establish procedures for reviewing, renegotiating and revising existing contracts, and
- Establish procedures for negotiating and executing new contracts when contracts are not in place or are about to expire.

Certain parties that may have incidental access to PHI, such a facility-cleaning contractor, are not business associates. Nevertheless, the covered entity should create a process for incorporating strong confidentiality provisions in agreements with these vendors.

### **Breaches of Contract**

Once contracts meeting the requirements of Section 164.504(e)(1) are in place, each covered entity will need to develop policies and procedures to act upon breaches of contract terms. While the Final HIPAA Privacy Rule as Modified does not require active monitoring of business associates, a covered entity is responsible for acting once a breach is brought to its attention. Likewise, the business associate is required to report any breaches on its part to the covered entity.

Pursuant to Section 164.504(e)(1)(ii), a covered entity is not in compliance with the Final HIPAA Privacy Rule as Modified if it knows of a “pattern of activity or practice of the business associate that constituted a material violation of the business associate’s obligations under contract...” and fails to take reasonable steps to cure the breach or end the violation. Reasonable steps may include terminating the contract, if feasible, or reporting the problem to the Secretary of Health and Human Services.

In its 07/06/01 Guidance on the Privacy Rule, HHS advised that a covered entity “is not liable for the privacy violations of a business associate” and that “covered entities are not required to actively monitor or oversee the means by which a business associate carries out safeguards or the extent to which the business associate abides by the requirements of the contract.” However, the covered entity is obligated to receive, and under certain circumstances, act upon reports that a business associate has breached its contractual requirements. As the Final HIPAA Privacy Rule as Modified provides little or no guidance as to the appropriate level of business associate oversight, covered entities will have to reach their own conclusions and establish policies and procedures to address monitoring business associates after consulting with counsel as to just how much investigation and monitoring or supervision, if any, of business associates will be appropriate for them, given the legal risks involved.

# Organizational Requirements - Group Health Plans

*Revision Date: 09/06/2002*

## Citations

The Final HIPAA Privacy Rule as Modified and its Preambles discuss the organizational requirements for group health plans in the following sections. In these sections, the term “Group Health Plan” is defined and the circumstances under which a Group Health Plan may disclose protected health information to a Plan Sponsor are prescribed.

- §160.103 - Definitions of “Group Health Plan” and “Plan Sponsor”
- §164.504(f) - Uses and Disclosures: Organizational Requirements for Group Health Plans
- §164.530(k) - Administrative Requirements: Group Health Plans
- Preamble to the Final Rule, pg. 82,507-09 - HHS Commentary on §164.504(f)
- Preamble to the Final Rule, pg. 82,563-64 - HHS Commentary on §164.530(k)
- Preamble to the Final Rule, pg. 82,645-48 - HHS Discussion of Public Comments on §164.504(f)
- Preamble to the Final Rule, pg. 82,750 - HHS Discussion of Public Comments on §164.530(k)
- Preamble to the Modifications, pg. 53,207 – 08 – HHS Commentary on Group Health Plan Disclosures of Enrollment and Disenrollment Information to Plan Sponsors

## General Rule

HIPAA covered entities include health care clearinghouses, health care providers and health plans. Specifically included within the "health plan" definition are “group health plans” (“GHP”) with 50 or more participants or those of any size that are administered by an entity other than the employer who established and maintains the plan. These group health plans may be fully insured or self-insured (or self-funded). Neither employers nor other group health plan sponsors, such as employee organizations, are defined as covered entities.<sup>2</sup>

The Employee Retirement Income Security Act of 1974 (“ERISA”), 29 U.S.C. §1001 et seq. generally regulates private sector GHPs. ERISA treats a GHP as an independent legal entity that must be managed by one or more fiduciaries and a plan administrator (29 U.S.C. §§ 1101-04, 1132). In contrast, Federal Employees Health Benefit (FEHB) plans meet the ERISA definition of “group health plan” but are regulated under the FEHB Act,

---

<sup>2</sup> The Privacy Rule defines ‘group health plans’ as “employee welfare benefit plans” under the Employee Retirement Income Security Act of 1974 (“ERISA”), § 3(1), 29 U.S.C. § 1002(1), offering “medical care” as further defined in the Public Health Service Act § 2791(a), 42 U.S.C. 300gg-91(a) and “plan sponsor” by reference to ERISA § 3(16)(B), 29 U.S.C. § 1002(16)(B).)

5 U.S.C. Ch. 89, rather than ERISA (see 29 U.S.C. § 1003(b)(1)) because they also meet ERISA’s definition of an exempted “governmental plan” (29 U.S.S. § 1002(32)).

The Final HIPAA Privacy Rule as Modified permits a plan sponsor to use two types of protected health information without satisfying any of the Rule’s requirements that are applicable to covered entities:

- A plan sponsor may perform GHP enrollment functions on behalf of its employees without using the standard transactions described in the HIPAA Transactions and Code Sets Standards.
- A plan sponsor also may receive from the GHP (or a health insurance issuer or an HMO with respect to a GHP) “summary information” to permit the plan sponsor either (a) to solicit premium bids from other health plans or (b) for the purpose of modifying, amending, or terminating the plan. According to §164.504(a), “summary information” summarizes claims history, claims expenses, or types of claims experienced by individuals for whom the plan sponsor has provided health benefits under a GHP, provided that specified identifiers listed in §164.514(b)(2)(i) are not included.

A unique set of rules applies to the situation where the plan sponsor requests that the GHP, or an insurer or HMO with respect to a GHP, disclose any other types of protected health information that the individual has not authorized under §164.508.<sup>3</sup> In that situation, the plan sponsor must agree to use and disclose the protected health information only for plan administration functions performed on the GHP’s behalf that are specified in ERISA-required plan documents, such as the summary plan description (“SPD”). These functions must be consistent with the Final HIPAA Privacy Rule as Modified. Furthermore, GHPs, and health insurance issuers or HMOs with respect to the GHP, that disclose protected health information to plan sponsors are bound by the minimum necessary standard as described in §164.514.

Thus, in order for the GHP to disclose to a plan sponsor protected health information – other than enrollment information or summary information – the appropriate authorized party named in the ERISA plan documents must amend the ERISA-required plan documents to:

- (1) Describe the permitted uses and disclosures of the protected health information;
- (2) Specify that disclosure is permitted only upon the GHP’s receipt of a certification from the plan sponsor that the plan documents have been amended and the plan sponsor has agreed to certain conditions regarding the use and disclosure of protected health information as required in §164.504(f)(2)(ii) (and are listed below); and
- (3) Provide adequate firewalls by identifying the employees or classes of plan sponsor employees who will have access to protected health information; restricting access solely to those employees identified and only for the functions performed on behalf of the group health plan; and providing a mechanism for resolving issues of noncompliance as required in §164.504(f)(2)(iii).

Consequently, any disclosure to plan sponsor employees or classes of employees not identified in those plan documents is an impermissible disclosure. To the extent a GHP has its own employees

---

<sup>3</sup> As GHPs often lack their own workforce, employers and other plan sponsors - particularly those sponsors with self-insured (or self-funded) GHPs – may use their employees to perform certain functions for the GHP and, in doing so, often require access to the GHP’s protected health information, thereby creating the situation where the plan sponsor must satisfy the requirements of § 164.504(f). Furthermore, if a GHP is not governed by ERISA, the plan sponsor and the GHP may not be separate legal entities in which case the hybrid entity rule should be invoked. See Organizational Requirements: Hybrid Entities.

separate from the plan sponsor's employees, they also are bound by the Privacy Rule's permitted uses and disclosures as the workforce of a covered entity.

The plan sponsor also must provide a certification to the GHP in which the plan sponsor agrees to:

- Not use or further disclose protected health information other than as permitted or required by the plan documents or as required by law;
- Ensure that any subcontractors or agents to whom the plan sponsor provides protected health information agree to the same restrictions and conditions;
- Not use or disclose the protected health information for employment-related actions or in connection with any other benefit or employee benefit plan of the plan sponsor;
- Report to the group health plan any use or disclosure that is inconsistent with the plan documents or the Final HIPAA Privacy Rule as Modified;
- Make the protected health information available to individuals in accordance with §164.524;
- Consider requests for amendment of protected health information in accordance with §164.526
- Provide an accounting of its disclosures in accordance with §164.528;
- Make its internal practices, books, and records available to the Secretary of Health and Human Services for determining compliance;
- If feasible, return or destroy all protected health information received from the GHP that the sponsor still maintains and retain no copies when no longer needed; if not feasible, limit further uses and disclosures to those purposes that make the return or destruction infeasible; and
- Ensure that the separation has been established as required in §164.504(f)(2)(iii).

HHS created this certification requirement to reduce the burden on health insurance issuers and HMOs. Without it, health insurance issuers and HMOs would need to review the plan documents in order to ensure that the amendments have been made before they could disclose protected health information to plan sponsors. According to HHS, the receipt of the certification is a sufficient basis for the health insurance issuer or HMO to disclose protected health information to the plan sponsor.

As part of the notice of privacy practices requirements in §164.520, group health plans that are subject to the §164.530 administrative requirements must inform participants that the plan may disclose protected health information to plan sponsors, including summary information. However, the plan sponsor is not required to provide the certification described above or amend plan documents in order to request and obtain summary information or enrollment information.

## **Policies and Procedures**

If a GHP fully insures its benefit offering through a health insurance issuer or an HMO and it does not create or receive protected health information other than summary information or enrollment information, then according to §164.530(k), it will not be obligated to prepare policies and procedures or fulfill any other Final HIPAA Privacy Rule as Modified administrative requirement other than the prohibitions against waiver of rights and retaliation or intimidation of persons who assert their rights. The GHP also is exempt from the notice of privacy practices and individual rights requirements because it does not have access to protected health information.

If a GHP self insures (or self funds) its benefit offering (or uses a combination of self-insurance and insurance such as a choice between fee-for-service and HMO coverage) or if it is an insured plan that requires protected health information beyond summary information or enrollment data, then the GHP will be obligated to create its own policies and procedures which would address permissible uses and disclosure to the plan sponsor and comply with all the other HIPAA administrative requirements. The plan administrator also may consider forming an Organized Health Care Arrangement. See Organizational Requirements: Organized Health Care Arrangements.

In any event, a health insurance issuer or an HMO must include in its policies and procedures a discussion on disclosures to GHPs and their plan sponsors, including the certification requirement. These organizations also will have to create a process for collecting the certifications and confirming that disclosures made to a particular GHP are consistent with the certification.

# Organizational Requirements - Hybrid Entities

*Revision Date: 09/06/02*

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss organizational requirements for hybrid entities:

- §160.103(2)(i) - Definition of health plan
- §164.501 – Definitions: Covered functions
- §164.504(a) – Definitions: Common Control, Common Ownership, Health Care Component, Hybrid Entity
- §164.504(b) - Standard: Health care component
- §164.504(c)(1) - Implementation specification: Application of other provisions
- §164.504(c)(2) - Implementation specifications: Safeguard requirements
- §164.504(c)(3) - Implementation specifications: Responsibilities of the covered entity
- §164.530(i) - Standard: Policies and Procedures
- §164.530(j) - Standard: Documentation
- Preamble to the Final Rule, pg. 82,475 and 82,567 – HHS Commentary on §160.103(2)(i) definition of health plan
- Preamble to the Final Rule, pg. 82,488 and 82,605 – HHS Commentary on §164.501 definition of covered functions
- Preamble to the Final Rule, pg. 82,502 and 82,637 – HHS Commentary on §164.504(a), §164.504(b), §164.504(c)(1), §164.504(c)(2), and §164.504(c)(3)
- Preamble to the Final Rule, pg. 82,563 and 82,748 – HHS Commentary on §164.530(i) and §164.530(j)
- Preamble to the Modifications, pg. 52,203–07 – HHS Commentary on Hybrid Entities

## General Requirements

The Final HIPAA Privacy Rule as Modified recognizes that certain covered entities may perform functions that are not covered functions under the Rule, or may manage many types of insurance products, some of which are considered excepted benefits and thus are not regulated by the Rule. Covered functions are functions that make an organization a health plan, health care provider, or health care clearinghouse within the Final HIPAA Privacy Rule as Modified's definitions (§160.103). Excepted benefits are insurance products that are excluded from the definition of health plan, such as workers compensation or life insurance, and thus are not regulated by the Final HIPAA Privacy Rule as Modified (Preamble page 82502; §160.103(2)(i) under the definition of health plan). Additionally, the Final HIPAA Privacy Rule as Modified recognizes

that single legal entity may perform functions that are both covered and non-covered under the Final HIPAA Privacy Rule as Modified by introducing the concept of “hybrid entity.”

A single legal entity that is a covered entity and is engaged in activities that are not covered functions may designate its “health care component(s) as a hybrid entity subject to the Final HIPAA Privacy Rule as Modified. Only designated health care components of the organization must comply with the Final HIPAA Privacy Rule as Modified. Examples include insurance companies that have lines of business that include health insurance but also are engaged in non-covered functions such as property and casualty or general liability insurance; or a company that is engaged in a non-health business but has a health clinic on-site.

If a covered entity designates health care components, it must include any component that would be a covered entity if it were a separate legal entity. The hybrid entity has the option of including components that would be business associates of covered entities if they were separate legal entities.

The following elements are required for hybrid entities:

- There must be adequate separation (i.e., firewalls) between the health care components of the entity and the other components.
- The covered entity must ensure that the health care component complies with the applicable safeguard requirements of the rule (§164.504(c)(2)), including:
  - The health care component does not release protected health information to another component of the covered entity if release would be prohibited under the rule if the health care component and other component were distinct legal entities (§164.504(c)(2)(i)).
  - The health care component must ensure the compliance with the Final Privacy Rule as Modified of any component part of the hybrid that performs covered functions, and any component part performing functions that would make such component a business associate if the two components were separate legal entities (§164.504 (c)(2)(ii)).
  - Any member of the workforce that performs duties for both the health care component and other components of the hybrid entity, must not use or disclose protected health information from the health care component of their work in a way prohibited by the Final HIPAA Privacy Rule as Modified (§164.504(c)(2)(iii)).
- The covered entity must comply with the policy and procedure requirements outlined in §164.530(i), and thereby document compliance with the Final HIPAA Privacy Rule as Modified, including these safeguard requirements.
- The covered entity must document the designation of health care components of the hybrid entity and retain such documentation as required by §164.530 (j) in written or electronic form for six (6) years from date of creation or date when it was last in effect, whichever is later.

## **Policies and Procedures**

Once an organization has determined that the concept of hybrid entity applies to itself, the specific policy and procedure requirements include:

- Only the health care component of the hybrid entity must comply with all Final HIPAA Privacy Rule as Modified requirements (§164.504 (b)), and

- A hybrid entity must document the designation of itself as a hybrid entity, and maintain documentation as required by §164.530 (j): in written or electronic form for six (6) years from date of creation or date when it was last in effect, whichever is later (§164.504 (c)(3)(iii)).

The covered entity that is a hybrid entity must ensure that:

There is adequate separation (i.e., the organizational equivalent of firewalls) between the health care components of the entity and the other components. The health care component may not release protected health information to another component of the covered entity if release would be prohibited under the Final HIPAA Privacy Rule as Modified if the health care component and other component were distinct legal entities;

- The health care component is in compliance with the Final HIPAA Privacy Rule as Modified for any component part of the hybrid that performs covered functions, and any component part performing functions that would make such component a business associate if the two components were separate legal entities; and
- Any member of the workforce that performs duties for both the health care component and other components of the hybrid entity, does not use or disclose protected health information from the health care component of their work in a way prohibited by the Final HIPAA Privacy Rule as Modified. [§163.504 (c)(2)]

A hybrid entity must comply with the standards and implementation specifications related to policies and procedures. Policies and procedures must be reasonably designed taking into account the size of and type of activities that relate to protected health information undertaken by the covered entity. The policies and procedures must change in concert with changes in the law or changes in the entity's privacy practices (§164.530(i)).

A hybrid entity must comply with the policy and procedure documentation retention requirement. Policies and procedures may be in written or electronic form and must be retained for six (6) years from date of creation or date when it was last in effect, whichever is later (§164.530(j))

# Organizational Requirements – Organized Health Care Arrangements

*Revision Date: 09/06/2002*

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss organizational requirements for organized health care arrangements.

The term “Organized Health Care Arrangement” (OHCA) is defined and the circumstances under which certain covered entities may form an OHCA and the benefits of forming an OHCA are identified in the following sections of the Final HIPAA Privacy Rule as Modified, 45 CFR Parts 160 and 164 and its Preambles:

- §160.103 – Definitions of “Business Associate” and “Health Plan”
- §164.501 – Definitions of “Health Care Operations” and “Organized Health Care Arrangement”
- §164.506(c)(5) – OHCA permissible sharing of PHI for Health Care Operations
- Preamble to the Final Rule, pg. 82,475-80 – HHS Commentary on §160.103 Definitions of “Business Associate” and “Health Plan”
- Preamble to the Final Rule, pg. 82,489-91, 494-95 – HHS Commentary on §164.501 Definitions of “Health Care Operations” and “Organized Health Care Arrangements”
- Preamble to the Final Rule, pg. 82,513 – HHS Commentary on §164.506(f)
- Preamble to the Final Rule, pg. 82,552 – HHS Commentary on §164.520(d)
- Preamble to the Final Rule, pg. 82,607-10 – HHS Discussion of Public Comments on §164.501 Definition of Health Care Operations
- Preamble to the Modifications, pg. 52,241-19 – HHS Discussion of Disclosures for Treatment, Payment, or Health Care Operations of another Entity

## General Rule

The Final HIPAA Privacy Rule as Modified allows legally separate covered entities that are integrated clinically or operationally to be considered an OHCA for compliance purposes if protected health information must be shared among the covered entities for the joint management and operations of the arrangement. The Final HIPAA Privacy Rule as Modified generally treats an OHCA as a covered entity for the purposes of contracting with business associates (§160.103 (Definition of “Business Associate”)) and of issuing and joint notices of privacy practices (§164.520(d)). It is reasonable to conclude that an OHCA also may develop a joint authorization under Section 164.508. The Final HIPAA Privacy Rule as Modified also includes within the scope of “Health Care Operations” the sharing of Protected Health Information among covered entities participating in an OHCA (§164.506(c)(5)). Consequently, covered entities participating in an OHCA do not have to obtain business associate agreements from one another with respect to the OHCA’s protected health information.

Section 164.501 of the Final HIPAA Privacy Rule as Modified (definition of OCHA) expressly recognizes the following types of OCHAs:

- (1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
- (2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
  - (i) Hold themselves out to the public as participating in a joint arrangement; and
  - (ii) Participate in joint activities that include at least one of the following:
    - (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
    - (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
    - (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
- (3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
- (4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
- (5) The group health plans described in paragraph (4) [above] and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

The Preamble to the Final Rule (pg. 82,494) identifies the hospital setting as a common example of the first type of OHCA and the independent practice association (IPA) as a common example of the second type. The other types of OHCA provide flexibility to plan sponsors who utilize an insurer or HMO or offer several group health plans. An OHCA is distinguishable from an affiliated covered entity arrangement (“ACE”) under section 164.504(d) of the Privacy Rule because the organizations participating in an OHCA do not have to be under common ownership or common control. See Organization Requirements: Affiliated Covered Entities.

## **Policies and Procedures**

The Final HIPAA Privacy Rule as Modified does not contain an implementation specification on forming an OCHA. Nevertheless, covered entities that choose to form an OHCA should confirm their decision in a written understanding (or an amendment to pre-existing organizational documents) that establishes the OCHA’s operational structure and defines the legal obligations of the participating organizations, such as mutual indemnification and insurance. These covered entities also should reflect the existence of the OHCA in their policies and procedures, particularly in the sections concerning permissible uses and disclosures, and notices of privacy practices, and

business associate contracting. See Business Associates, Permissible Uses and Disclosures, and Notices of Privacy Practices for more details.

# Preemption of State Law

Revision Date: 09/06/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address the issue of preemption of state law:

- §160.201 – Applicability
- §160.202 – Definitions
- §160.203 – General rule and exceptions
- §160.204 – Process for requesting exception determinations
- §160.205 – Duration of effectiveness of exception determinations
- Preamble to the Final Rule, pg. 82581, 82583 – Discussion of comments regarding preemption of state laws

## General Rule

Section 160.203 states that a standard, requirement, or implementation specification adopted under the Final HIPAA Privacy Rule as Modified that is *contrary* to a provision of State law preempts or supercedes that State law. Section 160.202 defines the *italicized* terms as follows:

- *Contrary* refers to instances where it would be impossible for a covered entity to comply with both the State and federal requirements or where the State law is an obstacle to accomplishing and executing the federal law.

*State law* refers to a constitution, statute, regulation, rule, common law, or other State action that has the force and effect of law.

### Exceptions to the General Rule

Section 160.203 also identifies the following exceptions to this general preemption rule:

- The Secretary of HHS has made a written determination under §160.204 that the provision of State law is necessary to
  - Prevent health care fraud and abuse;
  - Ensure regulation of insurance and health plans;
  - For State reporting on health care delivery or costs;
  - Serve a compelling need related to public health, safety or welfare; or
  - Serve the principal purpose of regulating controlled substances, or
- The State law that *relates to the privacy of individually identifiable health information* and is *more stringent* than a standard, requirement, or implementation specification adopted under the Final HIPAA Privacy Rule as Modified, or

- The State law is necessary for reporting, surveillance, investigation or intervention in matters of public health, or
- The State law pertains to monitoring, licensure or certification of facilities and individuals.

Section 160.202 defines the *italicized* terms as follows:

*More stringent* refers to the situation in which the State law restricts a use or disclosure that would be permitted under the federal law, or in which the State law allows greater access and amendment of an individual to his/her own personal health information, or has a consent process. In general, *more stringent* means greater privacy protection for the individual.

*Relates to the privacy of individually identifiable health information* means that the State law has the specific purpose of protecting privacy or affecting the privacy of health information in a direct way.

Section 160.204 describes the process for requesting a State exception to preemption from the Secretary of HHS. The State's chief elected official must make a written request to the Secretary. The request must identify the State making the request, name the specific requirement for which the exception is being requested, how health care providers, health plans, and other entities would be affected by the exception and list the reasons why the exception should be granted.

Section 160.205 states that an exception that has been granted is effective until either the State law or the federal standard are changed, or the exception is revoked.

The provisions requiring deference to state law relating to minor consent to health care and parental access to minor health care records are found in Section 502(g)(3).

## **Policies and Procedures**

While no specific policies or procedures are specified in the rule regarding preemption, state laws potentially affect all areas of a covered entity's Privacy Policies and Procedures. It is important to review applicable state laws when formulating any policy or procedure. In the event a state law does not specifically address an area of concern, it is a good practice to document that fact and the underlying Policies and Procedures rationale.

The covered entity also must consider the interplay between the HIPAA preemption scheme and other federal preemption schemes such as those found in the Medicare Act and the Employee Retirement Income Security Act of 1974. HHS advised in the Preamble that in the event of a conflict the pre-existing preemption schemes, Medicare and ERISA, would prevail over the HIPAA scheme.

Finally, covered entities that do business in multiple jurisdictions must assess choice of law issues.

## **Resources**

WEDI SNIP has developed other papers on the preemption issue that can be found at <http://snip.wedi.org>.

In 1999, the Georgetown University Health Privacy Project prepared a comprehensive survey of state health privacy laws that is currently in the process of updating. This report can be accessed at the Health Privacy Project web site at <http://www.georgetown.edu/research/ihcrp/privacy/statereport.pdf>.

# Administrative Requirements

# Administrative Requirements - Changes in Law

Revision Date: 09/09/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address the issue of changes to policies and procedures necessitated by changes in law:

- §164.530 (i)(3) – Changes in law: Implementation Specification – Standard: Policies and Procedures
- §164.520 (b)(3) – Revision to notice: Implementation Specification: Content of notice – Standard: Notice of Privacy Practices
- Preamble, pg. 82563 and 82748 – Changes in Policies and Procedures

## General Requirements

In section 164.530 (i)(3), the HIPAA Privacy Rule establishes the standard for changes to policies when there are changes in the 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.”

In section 164.520 (b)(3), the HIPAA Privacy Rule establishes requirements for revisions to the notice of privacy practices for protected health information:

“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.”

## Policies and Procedures

The preamble to the HIPAA Privacy Rule states that covered entities are required to modify their policies and procedures promptly to comply with changes in relevant law and, if changes also affect the practices stated in the notice, to change the notice. The preamble notes that nothing in the requirements regarding changes to policies and procedures or changes to the notice may be used by a covered entity to excuse a failure to comply with applicable law.

Under section 164.530 (i)(3), if changes in the law necessitate changes to the covered entity’s policies or procedures, the covered entity must promptly document and implement the revised policy and procedure.

If a change in the law materially affects the content of the notice required by section 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with section 164.520 (b)(3).

Section 164.520 (b)(3) requires that the covered entity 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
- 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 (preamble, pg. 82563).

# Administrative Requirements - Complaint Process

Revision Date: 09/09/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address requirements for a complaint process and the policies and procedures needed to implement these requirements:

- §160.306 – Complaints to the Secretary
- §160.310 (b), (c) – Responsibilities of covered entities to cooperate with complaint investigations and compliance reviews
- §160.312 – Secretarial action regarding complaints and compliance reviews
- §164.504(e)(2)(ii)(H) – Uses and disclosures of protected health information: general rules – Standard: Business associate contracts
- §164.530 (a)(1)(ii) – Administrative requirements – Standard: Personnel designations
- §164.530 (d) – Administrative requirements – Standard: Complaints to the covered entity
- §164.530 (g) – Administrative requirements – Standard: Refraining from intimidating or retaliatory action
- §164.520 (b)(1)(vi) – Notice of privacy practices for protected health information – Complaints
- §164.524 (d)(2)(iii) – Access of individuals to protected health information – Implementation specifications: Denial of access
- §164.526 (d)(1)(iv) – Amendment of protected health information – Implementation specifications: Denying the amendment
- Preamble, pg. 82487 – Process of filing a complaint
- Preamble, pg. 82505 – Complaints against a business associate
- Preamble, pg. 82550 – Information on complaints in notice of privacy practices
- Preamble, pg. 82556 – Review of a Denial of Access
- Preamble, pg. 82561 – Designation of Privacy Official and Contact Person
- Preamble, pg. 82562 – Complaints to the covered entity
- Preamble, pg. 82600-1 – Process for filing complaints
- Preamble, pg. 82746-7 – Complaints to the covered entity, retention of complaint records, and staffing requirements
- Preamble, p. 82783 – Internal Complaints

## General Requirements

The HIPAA Privacy Rule establishes the right of any person to file a complaint either directly with a covered entity (internal complaint) or with the Secretary of Health and Human Services. Covered entities must cooperate with investigations by the Secretary, providing access to information requested by the investigator. In addition, a covered entity's privacy notice must clearly explain how an individual may file a complaint with the covered entity and that the covered entity will not retaliate against any individual who files a complaint. Complaints filed by individuals directly with the Secretary must be made in writing, must name the entity against whom the complaint is lodged, must describe the acts or omissions and must be filed within 180 days of the time the individual became aware or should have been aware of the violation. However, the Secretary may waive timing requirements, if appropriate. Complaints may include violations of the covered entity's privacy practices and not just violations of the HIPAA Privacy Rule itself. Covered entities must receive and document complaints, but no response is required.

## **Policies and Procedures**

The Administrative Requirements section of the HIPAA Privacy Rule requires that a covered entity designate a contact person or office to be responsible for receiving complaints regarding its privacy practices. Covered entities must document any complaints and their disposition, if any, and retain these records for six years. Covered entities may not threaten, intimidate or retaliate against any individual who files a complaint.

### **Denial of Access**

If a covered entity denies an individual access to his/her protected health information, the covered entity must describe in its denial how the individual may complain to the Secretary and the covered entity. The description must include the name or title and telephone number of the person or office to which complaints may be made.

### **Denial of Amendment**

If a covered entity denies an individual's request to amend a medical record, the covered entity must explain in its denial how the individual may complain to the covered entity or to the Secretary. The description must include the name or title and telephone number of the person or office to which the complaint may be made.

### **Facilitating Investigations Arising From a Complaint**

If, as a result of a complaint to the Secretary of HHS, a covered entity is investigated, the covered entity must permit access to information during normal business hours (or at any time and without notice, if the Secretary determines that the circumstances warrant). Additionally, business associates of such covered entity are also required, pursuant to business associate agreements, to make information available to the Secretary for such investigations.

# Administrative Requirements - Designation of Privacy Official and Contact Person

*Revision Date: 09/09/2002*

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address designating a privacy official and contact person or office:

- §164.530(a) – Administration Requirements: Standard – Personnel designations
- §164.526(d)(1)(iv) – Amendment of protected health information – Implementation Specification – Denying the amendment
- Preamble, pg. 82561 – Administrative Requirements: Designation of a Privacy Official and Contact Person
- Preamble pg. 82563-64 – Standards for Certain Group Health Plans
- Preamble pg. 82595 – Federal Educational Rights and Privacy Act
- Preamble pg. 82744-45 – Designation of a Privacy Official and Contact Person
- Preamble pg. 82767-68 – Privacy Official

## General Requirements

A covered entity must designate a privacy official to be responsible for the development and implementation of the policies and procedures of the entity. A covered entity must also designate a contact person or office that is responsible for:

- Receiving complaints concerning the substance of policies and procedures adopted by a covered entity to comply with the HIPAA Privacy Rule;
- Receiving complaints concerning the covered entity's compliance with such policies and procedures or with the requirements of the HIPAA Privacy Rule generally; and
- Providing further information about matters covered by the notice of privacy practices required by §164.520 of the HIPAA Privacy Rule.

## Policies and Procedures

### Implementation Specification: Personnel Designations

A written or electronic record of the designation of the privacy official and the contact person/office must be maintained.

### Identity of Contact Person

The contact person may be, but is not required to be, the same individual as the privacy official. The choice in this regard is left to the discretion of the covered entity. HHS anticipates that the choice will often depend on the size and nature of the covered entity. In small organizations the function(s) may be under the auspices of a single part-time position; in large organizations there might be two full-time positions. The HIPAA Privacy Rule does not prescribe who within a covered entity must serve as the privacy official, does not prohibit combining this function with other duties, and does not prescribe any particular qualifications for the position. Duties may be delegated and shared, so long as there is one point of accountability for the covered entity's policies and procedures and compliance with the regulation.

### **Affiliated Entities**

In the case of affiliated entities, the number of positions necessary to comply with the privacy official/contact person requirements will depend on whether the entities are designated as a single covered entity or as separate covered entities. If a subsidiary is defined as a separate covered entity, a separate privacy official and contact person is required for that covered entity. If several subsidiaries are designated as a single covered entity, a single privacy official and contact person may be designated for the covered entity. If several covered entities participate in an “organized health care arrangement” and share a privacy notice with respect to services provided on the same premises, that notice need designate only one privacy official and contact person for the entities covered by that notice. Further, the HIPAA Privacy Rule permits the privacy official of one covered entity to serve as the privacy official of another covered entity, so long as all the requirements of the regulation are met for each such covered entity.

### **Group Health Plan**

A group health plan that provides benefits solely through an insurer or HMO, and that does not create, receive or maintain protected health information other than summary health information or information regarding enrollment and disenrollment, is not required to designate a privacy official or contact person/office.

# Administrative Requirements - Documentation

Revision Date: 09/09/2002

## Citations

Many sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address the administrative requirements for documentation:

- §164.508(b)(6) – Uses and disclosures for which an authorization is required
- §164.512(i)(2) – Uses and disclosures for research purposes
- §164.520(c)(2)(ii) – Notice of privacy practices for protected health information – Implementation specification: provision of notice (8/14/02)
- §164.520(e) – Notice of privacy practices for protected health information – Implementation specifications: Documentation
- §164.522(a)(3) – Rights to request privacy protection for protected health information
- §164.524(e) – Access of individuals to protected health information – Implementation specification: Documentation
- §164.526(f) – Amendment to protected health information – Implementation specification: Documentation
- §164.528(d) – Accounting of disclosures of protected health information – Implementation specification: Documentation
- §164.530(j) – Administrative requirements – Standard: Documentation
- Preamble, pg. 82517 – Retention of signed authorizations
- Preamble, pg. 82535-6 – Documentation Requirements of Internal Review Board or Privacy Board Approval of Waiver
- Preamble, pg. 82552 – Retention of copies of notices
- Preamble, pg. 82550 – Documentation of titles of persons or officers responsible for receiving and processing requests for amendments
- Preamble, pg. 82748 – Discussion of comments on documentation requirements for policies and procedures
- Preamble to the Modifications, pg. 53240 – Documentation requirements for acknowledgment of receipt of notice or good faith efforts to obtain acknowledgment

## General Requirements

The general standard, 164.530(j), requires that policies and procedures be documented either on paper or in electronic form. Any change to a policy, procedure or practice must also be documented. In addition to policies and procedures, privacy related communications, actions, decisions, activities or designations as well as any signed authorization must be documented and retained. The rule requires that all documentation be maintained for a period of six years.

## **Policies and Procedures**

As noted in the above section, the HIPAA Privacy Rule requires that the policies and procedures be maintained in writing, and that any other communication, action, activity, or designation that must be documented under this regulation be documented in writing, which may be in electronic form or on paper. This section highlights the major parts of the Privacy regulation where documentation requirements are specified. However, perhaps, the best principal for covered entities to use in determining whether to document an event or action is summarized in the following: The key to compliance with the HIPAA Privacy Rule lies in documentation.

Although numerous comments argued against requiring documentation, the final rule included this requirement. Requiring written documentation of key decisions about privacy is aimed at enhancing accountability, both within the covered entity and to the Department.

### **Documentation retention**

Documentation under the HIPAA Privacy Rule is required to be maintained for six years. While some believe the six-year retention period is too long and will pose undue cost to health care entities, this requirement was retained in the final rule because six years is the statute of limitations for the civil monetary penalties.

### **Notice of Privacy Practices**

A covered entity is required to provide adequate notice to an individual of the uses and disclosures of protected health information that it may make. A covered entity must document its compliance with the notice requirements by retaining copies of the notices it issues. In addition, providers with a direct treatment relationship with a patient are required to obtain an acknowledgment of receipt of its notice or must document and retain the provider's good faith efforts to obtain the written acknowledgment.

### **Right to request restriction of use and disclosure of protected health information**

A covered entity must permit an individual to request that the covered entity restrict uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations. The covered entity, however, is not required to agree with the restrictions, but if it does agree, it must document and strictly abide by the restrictions.

### **Access of individuals to protected health information**

An individual has a right of access to inspect and obtain a copy of protected health information about the individual for as long as the protected health information is maintained in the designated record set. A covered entity must document the designated record sets that are subject to access by individuals, and the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

### **Amendment of protected health information**

An individual has the right to request that a covered entity amend protected health information or a record about the individual for as long as the protected health information is maintained in the designated record set. The covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.

### **Accounting of disclosures of protected health information**

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. Covered entities must document and retain:

- The date of the disclosure;
- The name of the entity or person who received the protected health information and, if known, the address of such entity or person;
- A brief description of the protected health information disclosed;
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure;
- The written accounting that is provided to the individual, and
- The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

**Other general documentation requirements**

In addition to the requirements noted above, a covered entity must maintain documentation for:

- Any signed authorization;
- All complaints received, and their disposition, if any;
- Any sanctions that are applied as a result of non-compliance; and
- Any use or disclosure of protected health information for research without the individual's authorization.

# Administrative Requirements - Mitigation

*Revision Date: 09/09/2002*

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address the administrative requirements relating to mitigation:

- §164.530(f) – Administrative requirements – Standard: Mitigation
- Preamble, pg. 82562 - 63 and 82747-8 – Duty to Mitigate
- Preamble, pg.82641 – Responsibility to Mitigate Breaches by Business Associates

## General Requirements

Section 164.530 of the HIPAA Privacy Rule establishes standards under the general category of administrative requirements for covered entities. One such standard pertains to mitigation. In many cases the standards are accompanied by implementation specifications. However, there is no implementation specification for the mitigation standard.

## Policies and Procedures

Section 164.530(f) of the HIPAA Privacy Rule does not provide significant detail on the standard of mitigation. It simply states that “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.” However, a review of the preamble provides some insight. For example, at page 82748, the preamble clarifies that the regulation does not prescribe what mitigation policies and procedures must be implemented, and requires the covered entity to mitigate harm only where the covered entity has actual knowledge of harm. Further reducing the burden of the rule, the rule requires mitigation “to the extent practicable.” It does not require the covered entity to eliminate harm unless that is practicable. For example, if protected health information were inadvertently provided to a third party without authorization in a domestic abuse situation, the covered entity might have to promptly contact the patient as well as appropriate authorities and apprise them of the potential danger.

The preamble (page 82748) goes on to say that the duty to mitigate applies regardless of whether the privacy breach was caused by a member of the covered entity’s workforce, or by a contractor, as the harm to the individual is the same in either case. The covered entity is expected to take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to the patient or another individual, and what steps can actually have a mitigating effect.

In the discussion of comments to the proposed regulations, the preamble (page 82748) emphasizes flexibility and judgment by those familiar with the circumstances to dictate the best approach to mitigation.

# Administrative Requirements - Sanctions By Covered Entities Against Members of Its Workforce

Revision Date: 09/09/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss requirements related to sanctions by a covered entity against members of its workforce:

- §164.502(j)(1) – Disclosures by whistleblowers
- §164.502(j)(2) – Disclosures by workforce members who are victims of a crime
- §164.530(e)(1) – Standard: Sanctions
- §164.530(e)(2) – Implementation specification: Documentation
- §164.530(g) – Standard: Refraining from intimidating or retaliatory acts
- §164.530(j) – Standard: Documentation
- Preamble, pg. 82501 – 82502 and 82636 – Disclosures by Whistleblowers and Workforce Member Crime Victims
- Preamble, pg. 82562 and 82747 – Sanctions
- Preamble, pg. 82748 – Refraining from Intimidating or Retaliatory Acts

## General Requirements

Section 164.530 of the HIPAA Privacy Rule establishes standards and related implementation specifications under the general category of administrative requirements for covered entities. One such standard and implementation specification pertains to sanctions against the workforce of a covered entity.

Section 164.530(e)(1) states that a covered entity must establish and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or with the requirements of the regulations. This section does not cover the subject of sanctions taken by the regulator against the covered entity.

This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and meet the conditions of §164.502(j) [disclosures by whistle blowers or victims of crime] or §164.530(g)(2) [disclosures in pursuit of HIPAA enforcement]. Section 164.530(e)(2) establishes an implementation specification for documentation. It states that as required by §164.530(j), a covered entity must document the sanctions that are applied, if any.

## Policies and Procedures

A review of the preamble to the HIPAA Privacy Rule provides some insight into the above referenced standard and implementation specification. It indicates that covered entities are required to develop and impose sanctions appropriate to the nature of the violation. For example, the type of sanction would vary depending on factors such as the severity of the violation, whether the violation was intentional or

unintentional, and whether the violation indicated a pattern of improper use or disclosure of protected health information. Sanctions could range from warning to termination.

HHS states in the preamble to the HIPAA Privacy Rule that it believes it is important for the covered entity to have sanction policies documented so that employees are aware of what actions are prohibited and punishable. HHS does not define the particular sanctions that covered entities must impose. HHS indicates that training should be provided and expectations should be clear so individuals are not sanctioned for doing things that they did not know were inappropriate or wrong. HHS leaves the details of the sanctions policies to the discretion of the covered entity because the covered entity will be familiar with the circumstances of the violation and the best way to improve compliance.

HHS also requires covered entities to have written policies and procedures for the application of appropriate sanctions for violations, and to document those sanctions. However, a covered entity is not required to impose sanctions for disclosures by whistleblowers or workforce member crime victims, if those disclosures comply with the provisions of §164.502(j). In addition, complaints, investigations, or opposition that meet the provisions of §164.530(g)(2) are not subject to sanctions. These are the only exceptions.

### **Exceptions to Applying Sanctions to Workforce Members**

#### **Whistleblower Exception**

This exception is discussed in subsequent sections of these materials.

- Crime Victim Exception
- Complaints, Investigations and Opposition Exceptions

The exception in §164.530(g) states that a covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals and others who:

- File a complaint with the secretary of HHS under subpart C of part 160;
- Testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
- Oppose any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice is unlawful, and the manner of the opposition is reasonable and does not involve disclosure of protected health information in violation of this subpart.

# Administrative Requirements - Safeguards

*Revision Date: 10/23/2002*

## Citations

The following sections the Final Privacy Rule as Modified and the Privacy Rule preambles discuss safeguards:

- §164.502(a)(1)(iii) – Permitted uses and disclosures
- §164.530(c) – Standard: safeguards
- Preamble to the HIPAA Privacy Rule, pg. 82561 - 82562
- Preamble to the Modifications to the HIPAA Privacy Rule, pg. 53193 – 53195

## General Requirements

Section 164.530(c) requires that covered entities have in place “appropriate administrative, technical and physical safeguards to protect the privacy of protected health information.” Furthermore, section 164.502(a)(1)(iii) (which permits uses and disclosures that may occur incidental to an otherwise permitted use or disclosure) makes the acceptability of incidental uses and disclosures contingent upon the covered entity having implemented the safeguards required by §164.530(c), and the requirements under the “minimum necessary” standard (see section on Use and Disclosure – Minimum Necessary).

The exact nature of the safeguards that must be implemented are not specified. In the preamble to the HIPAA Privacy Rule, pg. 82562, the department of Health and Human Services says, “We do not prescribe the particular measures that covered entities must take to meet this standard...” They further note that the safeguards that should be implemented “...will vary with the size of the covered entity and the type of activities that the covered entity undertakes.” This ambiguity is considered to be consistent with the other efforts to make the HIPAA Privacy Rule “scalable”.

The only examples of safeguards that are specifically mentioned in the preamble to the HIPAA Privacy Rule are:

- Shredding documents prior to disposal.
- Requiring doors to medical records departments, or locking cabinets where medical records are kept, and limiting access to the keys or combinations to such locks.

Even these safeguards, however, are not mandated by the rule, but merely offered in the preamble as examples of what might be appropriate. To determine what is “appropriate” for a given covered entity, once again the department uses the standard of “reasonableness”. The preamble to the Modifications to the HIPAA Privacy Rule, pg. 53194, notes that “Each covered entity should assess the nature of the protected health information that it holds, and the nature and scope of its business, and implement safeguards that are reasonable for its particular circumstances.”

The HIPAA Security Rule (which at the writing of this paper has not been finalized but exists as an NPRM) will most likely set more definitive standards. However, the department has made it clear that covered entities must not wait for the final HIPAA Security Rule before making their own assessment of what safeguards are reasonable for their circumstances, and are appropriate to safeguard PHI. In the preamble to the Modifications to the HIPAA Privacy Rule, pg. 53194, the department notes “There should be no potential for conflict between the safeguards required by the Privacy Rule and the final Security Rule standards”.

Many individuals and entities have expressed concerns about the ambiguity of this standard. How can an entity know they have employed enough safeguards to prevent any improper use or disclosure and avoid any fines that may be imposed under the HIPAA Privacy Rule? How can an entity know that they are not wasting resources employing safeguards that are not required (or will not be required by the final Security Rule) or not necessary to safeguard PHI?

It may be impossible to answer such questions with any degree of certainty, but the HIPAA Privacy Rule does not require certainty and the preambles acknowledge this issue. The preamble to the HIPAA Privacy Rule, pg. 82562, notes that “Theft of protected health information may or may not signal a violation of this rule, depending on the circumstances and whether the covered entity had reasonable policies to protect against theft.” The preamble to the Modifications to the HIPAA Privacy Rule, pg. 53194, notes “...the fact that an incidental use or disclosure occurs does not by itself imply that safeguards were not reasonable.” The HIPAA Privacy Rule “...only requires that the covered entity reasonably safeguard protected health information to limit incidental uses or disclosures, not that the covered entity prevent all incidental uses and disclosures.”

## **Policies and Procedures Recommended to Implement the Standard**

As the subject of this white paper is policies and procedures, it will not attempt to address the physical or technical safeguards that covered entities should implement. While policies and procedures may themselves be considered administrative safeguards, one should not overlook that policies and procedures may be necessary to fully implement physical and/or technical safeguards. For example: locks on medical records rooms may be a physical safeguard but covered entities will most likely have to implement a policy that establishes when the medical records room will be locked and unlocked, and who will have access to the keys and/or combinations; user ID's and passwords to software systems may be technical safeguards but covered entities will most likely have to implement a policy that requires employees not share ID's and passwords, and periodically change passwords.

Because of the scalability of the standard, and the subjective nature of determining what is “reasonable”, it is impossible to prescribe exactly what policies and procedures a given covered entity may have to implement. As with the other safeguards, covered entities will have to perform their own assessment of what protected health information they hold, and determine what policies and procedures are reasonable to protect that information from improper use or disclosure.

The final HIPAA Security Rule may affect the policies and procedures that a covered entity needs to implement. Further guidance in this area may be available from the WEDI – SNIP Security Policies and Procedures white paper that has been written based on the HIPAA Security NPRM. This white paper will be revised once the final HIPAA Security is published.

# Administrative Requirements - Training For Staff

Revision Date: 09/09/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address the administrative requirements relating to training of a covered entity's workforce:

- §164.530 (b) – Administrative requirements – Standard: Training
- Preamble, pg. 82561 – Discussion of training requirements
- Preamble, pg. 82745 – Discussion of comments regarding training requirements

## General Requirements

In section 164.530(b), the HIPAA Privacy Rule establishes the general requirement that a covered entity provide training to its workforce with respect to protected health information:

*“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.”*

This section also establishes implementation specifications:

- The training must be provided to each member of the covered entity's workforce by no later than the compliance date for the covered entity.
- Thereafter, new members of the workforce must be provided training within a reasonable time.
- Training must be provided to each member of the covered entity's workforce whose functions are affected by a material change in the policies and procedures within a reasonable period of time after the material change becomes effective.
- A covered entity must document that the training has been provided.

## Policies and Procedures

The preamble to the HIPAA Privacy Rule and the review of comments discuss the requirements in §164.530(b) that a covered entity provide training for its workforce. The final HIPAA Privacy Rule eliminates both the requirement for employees to sign a certificate following training and the triennial recertification requirement. It requires that a covered entity provide training on the entity's policies and procedures to all members of the workforce as necessary and appropriate for them to carry out their functions. This training should be provided by the date on which the rule becomes applicable. After that date new members of the workforce should be provided training within a reasonable time after joining the entity. If a covered entity makes material changes to its policies and procedures, it is required to retrain members of its workforce whose duties are affected by the change within a reasonable period of time.

The covered entity must document that training has been provided. This can be done in written or electronic form and must be retained for six years. The methods or materials used in providing the training are not

specified. The discussion of comments also notes that although covered entities have a responsibility for breaches of privacy by their business associates, they are not required to monitor business associates' specific training procedures. However, a covered entity might consider including a training requirement in its business associate contracts as an appropriate means of protecting the health information provided to the business associate.

### **Policies and Procedures to Implement the Standard**

To implement the administrative requirement to provide training for its staff, the covered entity must:

- Determine the date on which it must be compliant;
- Develop methods and materials to provide the training;
- Develop policies and procedures to implement training for new members of its workforce;
- Develop policies and procedures to implement training for members of its workforce whose functions are affected by a material change in the entity's policies and procedures; and
- Develop a method to document the training in written or electronic form and maintain the documentation for six years.

# Administrative Requirements – Whistleblowers and Workforce Crime Victims

*Revision Date: 09/09/2002*

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss issues related to whistleblowers and workforce crime victims:

- §164.502(j) – Standard: Disclosures by whistleblowers and workforce member crime victims
- §164.512(f)(2)(i) – Listing of the protected health information that may be disclosed by a workforce member who is a victim of a crime
- §164.512(f)(5) – Crime on covered entity’s premises
- §164.530(e) – Sanctions
- Preamble, pg. 82501-02 and 82636-37 – Whistleblowers and workforce crime victims

## General Requirements

### Whistleblowers

A covered entity is not considered to have violated the requirements of the HIPAA Privacy Rule if a member of its workforce or a business associate discloses protected health information, provided that 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. In addition, the disclosure may only be made to:

- 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;
- 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;
- 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 covered entity’s conduct.

### Victims of a Crime

A covered entity is not considered to have violated the requirements of the HIPAA Privacy Rule 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:

- The protected health information disclosed is about the suspected perpetrator of the criminal act; and

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

## **Policies and Procedures**

The HIPAA Privacy Rule regulates covered entities, not members of a covered entity's workforce. In general, if a member of a covered entity's workforce makes an impermissible disclosure of protected health information, the HIPAA Privacy Rule makes the covered entity liable for that disclosure. However, there are two instances in which the HIPAA Privacy Rule provides that the covered entity will not be liable for a disclosure by a member of its workforce, even though the disclosure would otherwise be impermissible: a disclosure by a whistleblower, and a disclosure by a member of the workforce who has been the victim of a crime. In both instances, however, the covered entity is protected from liability only if the disclosure meets the requirements of the HIPAA Privacy Rule. Therefore, as part of the training required by the HIPAA Privacy Rule, it is important to explain to employees what may be disclosed by a whistleblower or a crime victim, and to emphasize that the circumstances in which such disclosures may be made are very limited.

The circumstances in which a whistleblower may disclose protected health information are limited to those in which the employee, in good faith, believes that his or her employer (the covered entity) has engaged in conduct which is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by the employer (covered entity) could potentially endanger one or more patients, workers or the public, and the disclosure is made to one of the entities listed in Section 164.502(j).

A crime victim is also limited as to what may be disclosed: the protected health information disclosed must be about the suspected perpetrator of the crime, and the disclosure must be limited to the information listed in Section 164.512(f)(2)(1).

In the training provided to its workforce, a covered entity may wish to include appropriate methods by which suspected violations by a covered entity can be reported. Options might include:

- Reporting violations to an immediate supervisor;
- Reporting violations to the covered entity's Compliance Officer; and
- Reporting violations through a hotline established specifically for the purpose of reporting violations.

The covered entity may wish to coordinate the training required by the HIPAA Privacy Rule with training that may be required by laws or regulations that require persons with certain kinds of information to disclose that information to the authorities.

# Individual Rights

# Individual's Rights - Accounting of Disclosures

Revision Date: 09/06/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss the individual's right to an accounting of disclosures:

- §164.502 – Uses and disclosures of Protected Health Information: general rules
- §164.508 – Uses and disclosures for which an authorization is required
- §164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required
- §164.514(e) – Standard: Limited data set
- §164.528 – Accounting of disclosures of Protected Health Information
- §164.530 (j) – Standard: Documentation
- Preamble to the HIPAA Privacy Rule, pg. 82513, 82517 – 82522, 82650, 82662 – 82663 –Uses and Disclosures for Which an Authorization Is Required
- Preamble to the HIPAA Privacy Rule, pg. 82524 and 82666 – Uses and Disclosures for Which Consent, an Authorization, or Opportunity To Agree or Object Is Not Required
- Preamble to the HIPAA Privacy Rule, pg. 82559 – 82561 and 82739 - 82744 – Accounting of Disclosures of Protected Health Information

## General Requirements

A covered entity is required to track all disclosures of protected health information that occur within a rolling six year window except for disclosures:

- For treatment, payment, or operations, as provided in §164.506;
- To the individual;
- That are incidental to a use or disclosure otherwise permitted or required, as provided for in §164.502;
- Pursuant to an authorization as provided for in §164.508;
- For facility directories, to people involved in an individual's care, or other notification purposes as provided for in §164.510;
- For national security or intelligence purposes as provided for in §164.512(k)(2);
- To law enforcement officials or correctional institutions as provided for in section §164.521(k);
- Of limited data sets, as provided for in §164.514(e); or
- That occurred prior to the compliance date for the covered entity.

This includes any disclosures that are made to or by any business associates of the covered entity. This may also include some disclosures that do not require the individual's authorization, as may be permitted by §164.512.

Individuals have the right to request an accounting of tracked disclosures (as defined above) made by a covered entity. This accounting must include all disclosures within the six years prior to the date of the request, or a shorter period if requested by the individual.

Disclosures made to health oversight agencies or law enforcement officials, as provided for in §164.512 (d) or (f) respectively, may be temporarily excluded from an accounting by a covered entity if the covered entity has been notified by such an agency or official that providing an accounting would impede the agency's or official's activities. Such notification should be given to the covered entity by the agency or official in writing and should specify the duration of the suspension. If the notification is made orally, then the covered entity must document the identity of the person who notified the covered entity, suspend the accounting of any subject disclosures, and limit the suspension to no more than 30 days from the date of the oral notification. If a written notification is subsequently submitted within that 30 day period, then the suspension may be extended as specified in the written notification. Once the time period requested for the suspension expires, the covered entity must include the disclosure in its accounting of disclosures.

### **Time to Respond to Requests**

Covered entities must provide an accounting of disclosures within 60 days of the request. Some states have defined a shorter period of time for response to requests and as such the state's shorter time requirement would prevail. If the covered entity cannot provide an accounting of disclosures within the 60-day period, it must provide a written statement to the requestor within the 60-day period specifying the reason for the delay and the expected completion date. The expected completion date may not be more than 30 days beyond the original 60-day period. Only one such extension is permitted per request.

### **Content of the Accounting of Disclosures**

The accounting must include the following information for each disclosure that was required to be tracked and that occurred within the accounting period (6 years prior to date of request or less, as specified by the requestor) including disclosures to or by business associates of the covered entity, as provided in §164.528(b):

- Date of disclosure;
- Name of covered entity or individual who received the information and their address if known;
- Description of information disclosed;
- Brief statement of the purpose of reason for disclosure, or in lieu of such a statement; a copy of a written request for a disclosure under §164.502(a)(2)(ii) or 164.512.

Multiple recurring disclosures to the same entity or individual or an authorization with multiple disclosures may have a summary entry. The summary entry requires all information as described above for the first disclosure, plus an indication of periodic interval, frequency, or total number of disclosures during the accounting period, and the date of last disclosure.

If during the accounting period the covered entity made disclosures as part of a research study, for fifty (50) or more individuals, the accounting provided to the individual may contain the following as an alternate to the requirements above:

- The name of the research protocol or activity;
- A description, in plain language, of the research protocol or activity, including the purpose of the research and criteria that were used to select records for inclusion;

- A description of the protected health information that was disclosed;
- The date or period over which such disclosures occurred or may have occurred, including the date of the last such disclosure during the accounting period;
- The name, address, and telephone number of the entity that sponsored the research and the researcher to whom the information was disclosed;
- A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or research activity.

If the covered entity does provide such a summary for disclosures that were part of a research protocol or activity, then the covered entity must, at the request of the individual, assist the individual in contacting the entity that sponsored the research, as well as the party conducting the research.

### **Fees for Providing Accountings of Disclosures**

Covered entities must provide one accounting within a rolling 12 month period, when requested, free of charge. A fee can be charged for any additional accounting requests within a rolling 12-month period. Such fees must be reasonable and based on the covered entity's cost incurred in preparing the accounting. If a fee will be charged, individuals must be informed of the amount of the fee in advance so they may amend their request to avoid or reduce the amount of the fee.

### **Documentation**

Covered entities are required to document and retain per section §165.630(j) the following:

- Information defined in Content of the Accounting of Disclosures section above;
- The written accounting provided to an individual requestor; and
- Titles of the person or offices responsible for receiving and processing accounting requests.
- Written documentation of an oral notification by a health oversight agency or law enforcement official to temporarily suspend an individual's right to an accounting of disclosures (pursuant to §164.528(a)(2)(ii)(A)).
- Any policies and procedures required to implement this standard.

### **Policies and Procedures**

A covered entity should:

- Develop policies and procedures as needed to ensure all disclosures that are required to be tracked are documented.
- Develop document retention policies to ensure such documentation of disclosures is saved for the required amount of time and available for inspection and audit as appropriate by authorized requestors.
- Develop a form for individuals to use to request accountings. The form should help ensure that all information necessary to process the request has been provided (e.g. how long a period does the individual want the accounting to cover?). The form may also be used to inform individuals of any applicable fees.
- Develop a procedure for processing requests for accountings. This procedure should:
  - Identify who receives requests;

- Establish the time allowed to respond to the request;
- Identify who will process the request, including determining what disclosures if any are not to be included in the accounting, and summarizing multiple disclosures to the same entity and/or for research protocols or activity;
- Establish the required contents of the final accounting to be delivered to the individual;
- Establish the means of delivering the accounting to the individual;
- Establishes when and how a fee will be collected.

# Individual's Rights - to Inspect and Copy

Revision Date: 09/06/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss the individual's right to inspect and copy protected health information:

- §164.524 – Access of individuals to Protected Health Information
- §164.530 (j) – Standard: Documentation
- Preamble to the HIPAA Privacy Rule, pg. 82554-8 – Access of Individuals to Protected Health Information
- Preamble to the HIPAA Privacy Rule, pg. 82731, and 82485 – Specifics regarding clinical lab exemptions and state laws that preempt this exemption

## General Requirements

An individual has a right of access to inspect and obtain a copy of protected health information (PHI) about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, except for:

- Psychotherapy notes<sup>4</sup>;
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
- PHI maintained by a covered entity that is 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 exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

### **Unreviewable grounds for denial §164.524(a)(2)**

A covered entity may deny an individual access without providing the individual an opportunity for review, if the information requested is:

- Psychotherapy notes;
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
- PHI maintained by a covered entity that is subject to the Clinical Laboratory exemptions (see above);
- If the covered entity is a correctional institution and if it would jeopardize the health, safety, security, custody or rehabilitation of an inmate or others;

---

<sup>4</sup> See definition of Psychotherapy notes at §164.501, pg. 82805

- Information created or obtained in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress provided the individual was previously informed of this and consents;
- For records that are subject to the Privacy Act, 5 U.S.C. §552a, access may be denied, if the denial of access would meet the requirements of that Act; or
- 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.

#### **Reviewable grounds for denial §164.524(a)(3)**

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)(3) of §164.524, in the following circumstances:

- 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;
- The PHI 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
- 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.

#### **Review of a denial of access §164.524(a)(4) and denial procedures §164.524(d)**

If access is denied on a ground permitted under §164.524 (a)(3) 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.

If the covered entity denies access, in whole or in part, to PHI, the covered entity must comply with the requirements of §164.524(d) which include:

- Making accessible any other requested information in the designated record set that the covered entity does not feel there are grounds to deny access to;
- The covered entity must provide a timely, written denial to the individual in plain language that must contain:
  - The basis for the denial;
  - If applicable, a statement of the individual's review; and
  - 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);
- If the covered entity does not maintain the PHI 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;

- 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.

### **Requests for access and timely action §164.524(b) and (c)**

§164.524(b) requires the covered entity to act on a request for access, within 30 days of receipt of the request, or 60 days if the information that needs to be access is stored off site. Covered entities may require that requests be submitted in writing. The covered entity may have a single extension of up to 30 days to respond to requests however, the covered entity must provide a written statement to the individual within the original deadline. This statement must explain the reason for the delay and the date by which the covered entity will respond to the request. Denials must be in writing.

§164.524(c) sets forth the procedures for access and allows a covered entity to charge reasonable fees, based on actual cost, for providing a copy of the PHI, if the individual agrees to the fees in advance. The covered entity must provide the access in the form or format requested by the individual. If it is not readily producible by covered entity in such form or format, the covered entity must provide a readable hard copy form or other such form as agreed by the covered entity and the individual.

The covered entity may provide the individual with a summary or explanation of the PHI requested instead of providing access if the individual agrees in advance to the summary or explanation and to fee the imposed, if any, by the covered entity for the summary or explanation.

### **Documentation §164.524(e)**

Covered entities are required to document and retain per section §165.630(j) the following:

- The designated record sets that are subject to access by individuals;
- The titles of the persons or offices responsible for receiving and processing requests for access by individuals;
- Any requests for access if required by the covered entity to be in writing;
- Any written denials to access;
- Any written statements to individuals establishing an extension to the response deadline.
- Any policies and procedures required to implement this standard.

### **Policies and Procedures Recommended to Implement the Standard**

- Develop a form for individuals to use to request access that assists him/her to provide complete information for the request
- Develop a policy that establishes the designated record sets that individuals will be permitted access to
- Develop a procedure for processing requests. This procedure should:
  - Establish how requests will be submitted (orally or in writing);
  - Identify who is responsible for receiving requests;
  - Establish the time allowed to process requests;
  - Identify who is responsible for reviewing the request to decide if access will be granted;
  - Establish the criteria that will be used to determine if access will be granted;

- Establish the process to notify the individual of the reply to the request;
- Establish the secondary review process and when it is needed;
- Establish the process to provide access or copies, including where access will be given, how records get to site if they are not stored at the facility, form and format that information will be provided in, when and how summaries will be used;
- Establish when and how a fee will be collected.

# Individual Rights - Notice of Privacy Practices

Revised 09/16/ 2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss the requirement for a notice of privacy practices:

- §164.520 – Notice of privacy practices for Protected Health Information
- §164.530 (j) – Standard: Documentation
- Preamble to the HIPAA Privacy Rule, pg. 82547-82552 – Notice of Privacy Practices for Protected Health Information
- Preamble to the HIPAA Privacy Rule, pg. 82720-82726 – HHS Discussion of Public Comments on Notice of Privacy Practices
- Preamble to the Modifications to the HIPAA Privacy Rule, pg. 53240– 53243 – HHS Discussion of the Final Modifications.

## General Requirements

Section 164.520 of the HIPAA Privacy Rule defines the right of an individual to receive a notice of a covered entity's privacy practices. This notice is intended to explain how the covered entity will use and disclose the individual's Protected Health Information (PHI) and to state the individual's rights and the covered entity's legal duties with respect to PHI (§164.520(a)(1)). This section also defines the requirements for a Notice of Privacy Practices. Covered entities are required to distribute their Notice of Privacy Practices and providers must make a good faith effort to obtain written acknowledgement of receipt from the individual. The following discussion refers to the Notice of Privacy Practices as the "Notice" and to PHI as "PHI".

### Exception for Group Health Plans

A group health plan ("GHP") that provides health benefits solely through an insurance contract with a health insurance issuer or HMO is not required to maintain or provide a Notice of Privacy Practices, so long as it does not create or receive PHI other than :

- Summary health information (as defined in §164.504(a)); or
- Information on whether an individual participates in the GHP or is enrolled in the health insurance policy or HMO that the GHP offers (§164.520(a)(2)(iii)).

However, if an insured GHP creates or receives PHI for other purposes, it must maintain a Notice of Privacy Practices and provide it upon request to any person. However, it need not send its Notice to all enrollees (§164.520(a)(2)(ii)).

A self-insured GHP must maintain and provide the Notice (§164.520(a)(2)(i)). At a minimum, the self-insured GHP's Notice must describe the plan's privacy practices with respect to the PHI it creates or receives through its self-insured arrangements. This Notice must be distributed to all participants in the self-insured arrangements and must also be available on request to other persons, including participants in the fully insured arrangements (preamble to the HIPAA Privacy Rule, pg. 82547-82548).

## **Inmates**

An inmate does not have a right to a Notice, and the HIPAA Privacy Rule's requirements respecting such Notices do not apply to a correctional institution that is a covered entity (§164.520(a)(3)).

## **Content of Privacy Notice**

The HIPAA Privacy Rule details the requirements for the Notice's content, but it does not include a model. The preamble to the HIPAA Privacy Rule (pg. 82548) explains that the requirements for the contents of the Notice set forth in the final regulation are not "exclusive," and that covered entities may include more information.

The preamble to the HIPAA Privacy Rule (pg. 82548) explains that a covered entity may be required, or may desire, to have more than one Notice. For example, a covered entity involved in a multi-state operation may need a different Notice for each state to reflect the different privacy requirements resulting from state laws that impose more stringent privacy requirements than are required under the regulation. A health care provider that is part of an organized health care arrangement and that also operates an independent practice may want to have different privacy practices for each entity, thus necessitating more than one Notice. In all cases, the Notice must accurately describe the privacy practices applicable to the persons receiving it. Furthermore, to the extent federal agencies are covered by HIPAA, they must comply with both the notice requirements of the Privacy Act of 1974 and the HIPAA Privacy Rule.

The preamble to the Modifications to the HIPAA Privacy Rule (pg. 53243) explains that a covered entity may utilize a "layered notice" where a short cover page that briefly summarizes the Notice is followed by longer and more detailed Notice. As long as all of the HIPAA Privacy Rule requirements for the content of the Notice in §164.520(b) are satisfied, the "layered notice" or any other format may be used.

## **Plain Language**

The HIPAA Privacy Rule requires that the covered entity write its notice in plain language so that the average reader can understand it (§164.520(b)(1)). The preamble to the HIPAA Privacy Rule (pg. 82548-82549) encourages covered entities to strive for clarity, make the notice available in languages other than English if a sizable portion of the population it serves is non-English speaking (even if not required to do so by law), and not to lose track of the fact that many people are unable to read.

## **Header**

The Notice must contain the following statement, either as a header or in some other way prominently displayed (§164.520(b)(1)(i)):

"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."

According to the preamble to the HIPAA Privacy Rule (pg. 82723), a covered entity may not combine the Notice with a consent or an authorization, but it may include the Notice in, or with, other documents that the covered entity shares with individuals "so long as the Notice is sufficiently separate."

If a covered entity chooses to use a consent form, it is permissible to design one form to include both the consent and the acknowledgement of receipt of the Notice. A consent is not required by the HIPAA Privacy Rule, but may be required by state law.

## **Uses and Disclosures**

The Notice must include:

- A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted to make under the HIPAA Privacy Rule for treatment, payment, and health care operations
- A description of each of the other purposes for which the HIPAA Privacy Rule permits or requires the covered entity to use or disclose PHI without the individual's written authorization
- A description of any material limitations or prohibitions imposed by state or other applicable law on permitted uses and disclosures for any purpose described in the preceding two bullets
- Sufficient detail in each such description to place the individual on notice of the uses and disclosures that are permitted or required by the HIPAA Privacy Rule and other applicable law
- 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 (§164.508(b)(5))

### **Separate Statements for Certain Uses or Disclosures**

If the covered entity intends to engage in any of the following activities, the description in the Notice must include a separate statement, explaining that:

- 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
- The covered entity may contact the individual to raise funds for itself; or
- A group health plan, or a health insurance issuer or HMO, may disclose PHI to the plan sponsor (§164.520(b)(1)(iii)).

### **Individual Rights**

The Notice must contain a statement of the individual's rights with respect to PHI and a brief description of how the individual may exercise these rights. The Notice must state the following rights:

- Right to request restrictions on certain uses and disclosures of PHI (accompanied by a statement that the covered entity is not required to agree to a requested restriction) §164.522(a);
- Right to receive confidential PHI communications of PHI §164.522(b);
- Right to inspect and copy PHI §164.524;
- Right to amend PHI §164.526;
- Right to receive an accounting of PHI disclosures §164.528;
- Right of an individual, including an individual who has agreed to receive the Notice electronically, to obtain a paper copy of the Notice upon request (§164.520(b)(1)(iv))

However, a covered entity may not limit its obligation to make a use or disclosure that either the law requires or the HIPAA Privacy Rule (§164.512(j)(1)(i)) permits to prevent or lessen a serious and imminent threat to the public or a person's health or safety (§164.520(b)(2)(i))

### **covered entity's Duties**

The Notice must explain the covered entity's duties to protect PHI (§164.520(b)(1)(v)) by including statements that:

- The law requires the covered entity to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI

- The law requires the covered entity to abide by the terms of the Notice currently in effect
- If the covered entity believes that, at some future date, it may wish to change a privacy practice that is described in the Notice it must include a statement that the covered entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains and a description of how it will provide individuals with a revised notice. (§164.520(b)(1)(v)(C). The preamble to the HIPAA Privacy Rule (pg. 82550-82551) emphasizes the importance of reserving this right in the Notice.

### **Complaints**

The Notice must contain a statement that individuals may complain to the covered entity and to the HHS Secretary if they believe their privacy rights have been violated, and it must include a brief description of how the individual may file a complaint with the covered entity and a non-retaliation statement (§164.520(b)(1)(vi)).

### **Contact**

The Notice must contain the name, or title, and telephone number of a person or office to contact for further information (§164.520(b)(1)(vii)).

### **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 published (§164.520(b)(1)(viii)).

### **Optional Elements**

If a covered entity decides to limit the uses or disclosures that it is permitted to make, 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).

For a the covered entity to apply a change in its more limited uses and disclosures to PHI, created or received before issuing a revised notice, the notice must include the statements required by §164.520 (b)(1)(v)(c).

### **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 (§164.520(b)(3)). If the Notice is revised, covered entities must make the revised Notice available upon request beginning on the revision's effective date. The preamble to the Modifications to the HIPAA Privacy Rule (pg. 53241) clarifies that the requirement to "revise and distribute" the Notice does not mean covered entities have to obtain a new acknowledgement of receipt (see the section on Provision of Notice for the requirements to obtain an acknowledgement of receipt).

### **Provision of Notice**

A covered entity must make the notice required by this section available on request to any member of the public (§164.520(c)). The intent is to enable prospective patients or enrollees to weigh a covered entity's

privacy practices in making his or her health care decision (preamble to the HIPAA Privacy Rule, pg. 82551, 82723).

A health care clearinghouse that creates or receives PHI other than as a business associate of a covered entity must produce a notice. If a health care clearinghouse creates or receives PHI only as a business associate of other covered entities, it is not required to produce a notice (preamble to the HIPAA Privacy Rule, pg. 82547).

### **Specific Requirements for Health Plans**

A health plan must provide its notice to its enrollees as follows:

- Not later than its HIPAA Privacy Rule compliance date
- To new enrollees at the time of enrollment
- A revised Notice must be provided to current enrollees within 60 days of a material revision to the Notice (§164.520(c)(1)(i))
- Furthermore, at least once every three years the health plan must notify its enrollees of the availability of the Notice and how to obtain the Notice (§164.520(c)(1)(ii))

A health plan will be compliant with these notice requirements if it provides its Notice to the named insured of a policy. It is not required to send the Notice to dependents (§164.520(c)(1)(iii)). Also, if a health plan has more than one notice, it should provide the Notice that is relevant to the individual requesting a copy (§164.520(c)(1)(iv)).

### **Specific Requirements for Health Care Providers**

A health care provider who has a direct treatment relationship with an individual must provide the Notice after the compliance date for the provider and no later than the first service delivery date or as soon as reasonably practical if the first service delivery date was an emergency treatment situation. First dates of service specifically include any service that may have been delivered electronically.

Except for emergency treatment situations, providers must make a good faith effort to obtain written acknowledgement from the individual that they received the Notice. If they cannot obtain such acknowledgement the provider must document their good faith effort and the reason they were unsuccessful.

The preamble to the Modifications to the HIPAA Privacy Rule provides examples of how providers might satisfy the “good faith effort” requirement, and of what constitutes the “first service delivery date” for certain situations.

The preamble to the Modifications to the HIPAA Privacy Rule states that a “good faith effort” to obtain written acknowledgement does not require the individual’s signature on the notice (pg.53240). The acknowledgement does have to be in writing but the provider otherwise has discretion to design the process that works best for their setting. The preamble to the Modifications to the HIPAA Privacy Rule specifically recognizes two possible methods: providing a tear-off cover sheet to the Notice that the patient signs and returns when they are given the Notice; or having the patient sign a log sheet or list that documents who has received the Notice. Documenting why a provider was unable to obtain an individual’s acknowledgement may be a simple as a written statement that the individual refused to sign the acknowledgement (if such was the case), signed by the employee who tried but failed to obtain the acknowledgement.

The preamble to the Modifications to the HIPAA Privacy Rule notes that if the first service was delivered by telephone then the provider must mail the Notice to the individual on the day of that call (pg. 53240). However, the preamble to the Modifications to the HIPAA Privacy Rule specifically notes that when the initial contact with a patient is a telephone call to schedule an appointment, providers may satisfy the Notice

delivery requirements by providing the Notice to the individual the next time they arrive at the office, for their appointment or otherwise (pg. 53240).

Although the HIPAA Privacy Rule includes detailed specifications about electronic delivery of the Notice, it does not specify how the paper version of the Notice may be delivered. In view of similar requirements under for example ERISA, first class U.S. Mail – but not third class or bulk mail -- delivery would be appropriate. Certified mail would not be required.

Health care providers who maintain a physical service delivery site are further required to have the Notice available for individuals to take with them, upon request, and to post the Notice in a prominent location where it is reasonable to expect that individuals seeking service will be able to read it.

### **Specific Requirements for Electronic Notice**

A covered entity that maintains a patient 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 (§164.520(c)(3)(i)).

A covered entity may provide the Notice 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 be deemed compliant if delivered within the time the HIPAA Privacy Rule specifies for paper notice (§164.520(c)(3)(ii)).

If a direct treating health care provider delivers the first service electronically, the provider must deliver electronic notice automatically and contemporaneously in response to the individual's first request for service (§164.520(c)(3)(iii)). A person who receives an electronic notice may still request a paper Notice (§164.520(c)(3)(iv)). The requirements for the provider to make a good faith effort to obtain written acknowledgement of the individuals receipt of the Notice do apply to Notices that are provided electronically (see section on Provision of Notice for the requirements to obtain written acknowledgement). The preamble to the Modifications to the HIPAA Privacy Rule note that “written acknowledgement”, in the case of Notices that have been provided electronically, do include electronic acknowledgements such as return receipts or other email acknowledgements.

### **Joint Notice by Separate Covered Entities**

Covered entities that participate in organized health care arrangements may comply with the Notice requirement by a joint notice, if:

- Each agrees to abide by the terms of the Notice with respect to PHI created or received by the covered entity as part of its participation in the organized health care arrangement;
- The joint Notice includes the required substance, except that the statements generally required by the HIPAA Privacy Rule may be altered to reflect the fact that the Notice covers more than one covered entity; reasonably describes the covered entities, or class of entities, to which the joint notice applies; reasonably describes the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and if applicable, states that the covered entities participating in the organized health care arrangement will share PHI with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement. (§164.520(d)(1) and (2)).
- The provision of Notice requirements will be satisfied if any one of the covered entities participating in the organized health care arrangement furnishes the Notice to an individual. (§164.520(d)(3)).

### **Documentation.**

Covered entities are required to document and retain per section §165.630(j) the following:

- Current and passed Notices of Privacy Practices issued by the covered entity;
- Written acknowledgements of receipt of Notice;
- Written documentation of good faith efforts that failed to obtain written acknowledgement.
- Any policies and procedures required to implement this standard.

## **Policies and Procedures**

To comply with requirements related to the notice of privacy practices, a covered entity should:

- Develop a Notice of Privacy Practices in plain language and evaluate the feasibility of a “layered notice” or other format to enhance readability.
- Develop a procedure to review/revise and retain the Notice of Privacy Practices (Notice) as changes occur.
- Establish a procedure to ensure individuals are provided the Notice no later than the first service delivery, what role is responsible and when in the admission/registration process is the Notice provided.
- Develop a form or log to obtain written acknowledgement of receipt of the Notice, or for employees to document their good faith efforts and why they failed to obtain written acknowledgement.
- Establish a procedure to follow-up in emergency circumstances when the Notice has not been provided.
- Establish a procedure to ensure the appropriate distribution of the Notice when new revisions are issued (e.g. new revision must be posted in waiting rooms, posted on web sites, provided to individuals upon request, provided to patients if they have not already received that version, etc.).

# Individual's Rights - Request Amendment

Revision Date: 09/06/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles address the individual's right to request amendment of protected health information (PHI):

- §164.524(a)(2)&(3) – Unreviewable and reviewable grounds for denial
- §164.526 – Amendment of Protected Health Information
- §164.530 (j) – Standard: Documentation
- Preamble to the HIPAA Privacy Rule, pg. 82558 – Amendment of Protected Health Information
- First Guidance on the HIPAA Privacy Rule 07/06/01 – Discussion of the Privacy Rule's requirements regarding patient access and the Clinical Laboratory Improvements Amendments of 1988 (CLIA)

## General Requirements

§164.526 states that an individual has the right to have a covered entity amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

A covered entity may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request:

- Was not created by the covered entity (unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment);
- Is for information that is not part of the designated record set;
- Would not be available for inspection under section 164.524(a)(2) or (3); or
- Is accurate and complete.

Sections 164.526(b) through (f) detail the technical specifications for implementation procedures and are paraphrased below.

### **Requests for amendment and timely action §164.526(b)**

The covered entity must permit an individual to request that the covered entity amend the PHI maintained in the designated record set. If the covered entity informs the individual in advance, the covered entity may require that individuals submit requests for amendment in writing and provide a reason to support the requested amendment.

The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of the request.

- If the covered entity grants the requested amendment, in whole or in part, it must take the actions as detailed in §164.526(b).
- If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial as detailed in §164.526(d).

If the covered entity is unable to act on the amendment within the time required above, the covered entity may extend the time for such action by no more than 30 days, provided that:

- The covered entity, within the time limit set forth above, 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
- The covered entity may have only one such extension of time for action on a request for an amendment.

#### **Accepting the amendment §164.526(c)**

If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements:

- **Making the amendment.** The covered entity must make the appropriate amendment to the PHI 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.
- **Informing the individual.** 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 as set forth below.
- **Informing others.** The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:
  - Persons identified by the individual as having received PHI about the individual and needing the amendment; and
  - Persons, including business associates that the covered entity knows have the PHI 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.

#### **Denying the amendment §164.526(d)**

If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements:

- **Statement of denial.** The covered entity must provide the individual with a timely, written denial. The denial must use plain language and contain:
  - The basis for the denial;
  - The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
  - 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 PHI that is the subject of the amendment; and
  - A description of how the individual may complain to the covered entity pursuant to the complaint procedures or to the Secretary, including the name, or title, and telephone number of the contact person or office designated to receive complaints.
- **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.

- **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.
- **Record keeping.** The covered entity must, as appropriate, identify the record or PHI 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.
- **Future disclosures.**
  - If the individual has submitted a statement of disagreement, the covered entity must include the material appended in accordance with the Record keeping section above, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.
  - 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 PHI only if the individual has requested such action.
  - When a subsequent disclosure described above 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 this section, to the recipient of the standard transaction

#### **Actions on notices of amendment §164.526(e)**

A covered entity that is informed by another covered entity of an amendment to an individual's PHI must amend the PHI in designated record sets.

#### **Documentation §164.526(f)**

Covered Entities are required to document and retain per section §165.630(j) the following:

- Any requests for access if required by the covered entity to be in writing;
- Any written denials to amendment;
- Any written statements to individuals establishing an extension to the response deadline;
- Any statements of disagreement submitted by the individual;
- Any statements of rebuttal submitted by the covered entity.
- Any policies and procedures required to implement this standard.

### **Policies and Procedures Recommended to Implement the Standard**

To implement the individual's right to request restriction of disclosures standard, the covered entity should:

- Develop a procedure to process requests for restrictions. This procedure should:
  - Establish the criteria to determine whether the request will be accepted or denied. The right to request restrictions should encourage discussions between the covered entity and the individual in

order to prevent restrictions that would not be in the best interest of the individual. Covered Entities are encouraged to discuss with individuals that the restricted information may be used or disclosed in emergency situations. The covered entity's ability to manage specific accommodations should also be considered.

- Establish the process for notifying individuals of acceptance or denial of the request;
- Establish how restrictions to which the individual and covered entity have agreed to will be documented and enforced. No specific form of documentation is required. A note in the medical record or similar notation is sufficient.
- Develop procedures to terminate a restriction. This procedure should:
  - Establish how to contact an individual with respect to the termination of an agreed to restriction;
  - Establish how to document the individual's agreement to the termination, if received;
  - Establish how to identify what information may still be subject to the restriction, even after the termination

# Individual's Rights - Request Confidential Communications

Revision Date: 09/06/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss the individual's right to request confidential communications.

- §164.502(h) – Standard: Confidential communications
- §164.522(b) – Standard: Confidential communications requirements
- §164.530 (j) – Standard: Documentation Requirements
- Preamble to the HIPAA Privacy Rule, pg. 82501, 82635 – Confidential Communications
- Preamble to the HIPAA Privacy Rule, pg. 82553 and 82729 - 82731 – Confidential Communications

## General Requirements

In the preamble to the HIPAA Privacy Rule, the discussion of comments regarding §164.522(a), notes that the final rule creates

*“A new provision, that provides individuals with a right to confidential communications. This provision grants individuals with a right to restrict disclosures of information related to communications made by a covered entity to the individual, by allowing the individual to request that such communications be made to the person at an alternative location or by an alternative means.”<sup>5</sup>*

A provider must accommodate any reasonable request for confidential communication and may not require an explanation of the reason for the request. It is not necessary that an individual be in an abusive situation to make a request for confidential communications. The provider may only require that the request be reasonable, that the request is put in writing and that the request specify an alternative address or method of contact and that (where applicable) the individual provides information on how payment for services will be handled. Modest additional cost to the provider is not considered to be unreasonable.

In the case of a health plan, an individual also has the right to request confidential communication. However, the health plan may require that an individual state that disclosure of confidential communications could endanger the individual. The right to request confidential communication applies to communications from the covered entity to the individual and also to communications that would otherwise be sent to the subscriber of an insurance policy under which the individual has coverage. An individual, for example, who does not want family members to know about a certain treatment, may request that the provider communicate with the individual about that treatment at the individual's workplace, by mail to an alternative address, or by phone to an alternative phone number.

The Privacy Rule requires that health care providers accommodate all reasonable requests for confidential communications. Health plans must accommodate all reasonable requests, if the individual clearly states that the disclosure of all or part of the protected health information (PHI) could endanger the individual.

---

<sup>5</sup> Federal Register /Vol.65, No.250/ Thursday, December 28, 2000/ Rules and Regulations, p. 82729.

The reasonableness of a request must be determined by a provider solely on the basis of the administrative difficulty of complying with the request. Covered entities are encouraged to establish policies and procedures to determine if a request for confidential information is considered reasonable:

- A covered health care provider or health plan cannot refuse to accommodate a request based on its perception of the merits of the individual's reason for making the request.
- A covered health care provider may not require the individual to provide a reason for the request as a condition of accommodating the request.
- If the individual indicates that the information will cause endangerment, the covered entity cannot further consider the individual's reason for making the request in determining whether it must accommodate the request.
- A covered health care provider or health plan may refuse to accommodate a request if the individual has not provided information as to how payment, if applicable, will be handled, or if the individual has not specified an alternative address or method of contact.

### **Documentation**

Covered entities are required to document and retain per section §165.630(j) the following:

- Written requests for confidential communications (if required by the covered entity)
- Any policies and procedures required to implement this standard.

### **Policies and Procedures**

Covered entities must develop procedures for processing requests for confidential communications. This procedure should:

- Establish how requests will be submitted (orally or in writing);
- Identify who is responsible for reviewing the request to decide if it will be accepted;
- Establish when information concerning payment for services will be required of the requestor;
- Establish the process to notify the individual of the reply to the request;
- Establish the process to document the alternate means of communication, communicate it to effected parties, and ensure future communications are consistent with the agreement.

# Individual's Rights - Request Restriction of Uses and Disclosures

Revision Date: 09/06/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss the individual's right to request restriction of uses and disclosures of protected health information (PHI).

- §164.522(a) – Standard: Right of an individual to request restriction of uses and disclosures.
- §164.530 (j) – Standard: Documentation
- Preamble to the HIPAA Privacy Rule, pg. 82552-3 – Discussion of §164.522(a)
- Preamble to the HIPAA Privacy Rule, pg. 82726-30 – Discussion of comments regarding §164.522(a)

## General Requirements

In §164.522(a), the HIPAA Privacy Rule establishes the general standard for the right of an individual to request restriction of uses and disclosures:

“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).”<sup>6</sup>

The preamble to the HIPAA Privacy Rule and the discussion of comments section discuss in detail the requirements in §164.522(a) for implementing the standard regarding the right of an individual to request restriction of uses and disclosures. The final rule gives individuals the right to request that a covered entity restrict the use or disclosure of protected health information (PHI) for treatment, payment, or health care operations. All covered entities must permit individuals to make this request. However, a covered entity is not required to agree to a restriction. If a covered entity does agree to a restriction, the covered entity and the covered entity's business associates must honor the restriction with two exceptions:

- It is terminated either by the covered entity or the individual. If the individual agrees to terminate the restriction, the covered entity may use and disclose PHI as otherwise permitted under the rule. If the covered entity terminates the restriction without the individual's agreement, it may only terminate the restriction with respect to PHI it creates or receives after the date it informs the individual of the termination.
- In an emergency treatment situation the standard allows the covered entity to use or disclose information to a health care provider for providing treatment. The covered entity must request that provider not further use or disclose the information.

## Documentation

---

<sup>6</sup> §164.510(b) is the standard that discusses uses and disclosures for involvement in the individual's care and notification purposes.

Covered entities are required to document and retain per section §165.630(j) the following:

- Any restrictions agreed to
- Agreement by an individual to terminate restrictions
- Any policies and procedures required to implement this standard.

## **Policies and Procedures**

To implement the individual's right to request restriction of disclosures standard, the covered entity should develop a procedure to process requests for restrictions. This procedure should:

- Establish the criteria to determine whether the request will be accepted or denied. The right to request restrictions should encourage discussions between the covered entity and the individual in order to prevent restrictions that would not be in the best interest of the individual. Covered Entities are encouraged to discuss with individuals that the restricted information may be used or disclosed in emergency situations. The covered entity's ability to manage specific accommodations should also be considered.
- Establish the process for notifying individuals of acceptance or denial of the request;
- Establish how restrictions to which the individual and covered entity have agreed to will be documented and enforced. No specific form of documentation is required. A note in the medical record or similar notation is sufficient.

The covered entity should also develop procedures to terminate a restriction. These procedures should:

- Establish how to contact an individual with respect to the termination of an agreed to restriction;
- Establish how to document the individual's agreement to the termination, if received;
- Establish how to identify what information may still be subject to the restriction, even after the termination

# Uses and Disclosures

# Use and Disclosures - Authorizations

Revision Date: 09/06/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy Rule preambles discuss the requirements for authorizations.

- §164.508(a) – Standard: authorizations for uses and disclosures
- §164.508(b) – Implementation specifications: general requirements
- §164.508(c) – Implementation specifications: core elements and requirements
- §164.508(d) – Implementation specifications: Authorizations requested by a covered entity for its own uses and disclosures
- §164.508(e) – Implementation specifications: Authorizations requested by a covered entity for disclosures by others
- §164.508(f) – Implementation specifications: Authorizations for uses and disclosures of Protected Health Information created for research that includes treatment of the individual
- §164.512 – Uses and disclosures for which an authorization, or opportunity to agree or object is *not* required
- §164.530 (j) – Documentation Requirements
- Preamble to the HIPAA Privacy Rule, pg. 82509-11 – Discussion of consents and the differences in consent and authorization
- Preamble to the HIPAA Privacy Rule, pg. 82513-21 – Discussion of authorizations

## General Requirements

Section 164.508 of the HIPAA Privacy Rule establishes the uses and disclosures for which an authorization is required. Covered entities must have authorization from individuals before using or disclosing protected health information (PHI) for any purpose not otherwise permitted or required by the HIPAA Privacy Rule. A valid authorization must be used only for the specific purpose(s) stated in the authorization and only by personnel listed in the authorization.

Situations in which covered entities are **NOT** required to obtain the individual's authorization to use or disclose PHI include:

- Treatment, payment, and health care operations
- Disclosures to the individual who is the subject of the information;
- Uses and disclosures of PHI permitted under §164.510 (uses and disclosures requiring an opportunity for the individual to agree or object) or 164.512 (uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required); and
- Required disclosures to the Secretary for enforcement of the rule.

The HIPAA Privacy Rule requires somewhat tighter restrictions concerning psychotherapy notes. An authorization is required for use and disclosure of psychotherapy notes except for the following uses:

- Use by the originator of the psychotherapy notes for treatment;
- 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; and
- Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual.
- Use or disclosure that is required or permitted by the HIPAA Privacy Rule with respect to the oversight of the originator of the psychotherapy note.

Authorizations are specifically required before a covered entity may make any use or disclosure for the purposes of marketing (as defined by the Modifications to the HIPAA Privacy Rule), except if the communication is in the form of:

- Face to face communication by a covered entity to an individual
- A promotional gift of nominal value provided by the covered entity

If a marketing communication involves any direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

The authorization form must be a separate form and cannot generally be combined with a consent form, except for specific instances such as for research involving treatment. If the individual does not understand what information is covered by the authorization, the use or disclosure is not permitted until the covered entity clarifies the request. There are no limitations on the information that can be authorized for disclosure.

If a class of entities is authorized to see information, the class must be defined so that a covered entity will know with reasonable certainty that the individual intended the covered entity to be included in the authorization. For example, an authorization for “all physicians” is probably not a good idea. A covered entity must document and retain any signed authorization and revocations must be submitted in writing and kept by the covered entity.

Section 164.512 details exceptions to the general requirement for authorizations for uses and disclosures including:

- Those required by law;
- For public health activities;
- About victims of abuse, neglect or domestic violence;
- For health oversight activities;
- For judicial and administrative proceedings;
- For law enforcement purposes;
- Those about decedents;
- For cadaveric organ, eye or tissue donation purposes;
- For research purposes;
- To avert a serious threat to health or safety;
- For specialized government functions; and
- For workers’ compensation.

### **Core elements required for all authorizations**

The authorization form must be written in plain language and include these core elements and required statements:

- A description of the information to be used or disclosed;
- The name of the covered entity, or class of entities or persons, authorized to use or disclose the Protected Health Information;
- The name or class of entities or persons to whom the covered entity may make the use or disclosure;
- A statement of the purpose of the use or disclosure. If the authorization is initiated by the individual, the statement “At the request of the individual” is adequate;
- An expiration date, time period or event. For authorizations for use or disclosure for a research study, the event may be defined as “end of the research study”, or “none”;
- A statement regarding the individual’s right to revoke the authorization and a description of how the individual may revoke the authorization or a reference to the covered entity’s Notice of Privacy Practices where such information is contained;
- A statement as to the ability or inability of the covered entity to condition treatment, payment, or enrollment upon the provision of an authorization (as may be permitted by the HIPAA Privacy Rule), including the consequences of refusal to sign the authorization;
- A statement that the information may be subject to re-disclosure by the recipient and may no longer be protected by the federal privacy law;
- The individual’s signature and date of signature; and
- If signed by a representative, a description of the representative’s authority to act for the individual and/or relationship to the individual.

### **Authorizations for an entity’s own uses and disclosure**

If a covered entity seeks an authorization for use and disclosures for its own purposes, a copy of the signed authorization must be made available to the individual.

### **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:

- An authorization for use and disclosures of PHI for research may be combined with other types of written permission for the same research study;
- 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; and
- An authorization, other than for psychotherapy notes, may be combined with another authorization except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations.

### **Defective authorizations**

An authorization is not valid if it has any of the following defects:

- The expiration date or event has passed;

- The authorization was not filled out completely;
- The authorization is revoked;
- The authorization violates any of the requirements regarding Compound Authorizations or Conditioning of Authorizations;
- The authorization contains material information known by the covered entity to be false.

### **Prohibition on conditioning of authorizations**

A covered entity may *not* condition provision of treatment, payment, enrollment, or eligibility for benefits on provision of an authorization except in the case of:

- Research related treatment;
- Pre-enrollment underwriting or risk determinations (excluding authorization for use or disclosure of psychotherapy notes);
- Provision of health care solely for the purpose of creating PHI for disclosure to a third party (e.g., pre-employment physicals).

### **Revocation of an authorization**

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:

- The covered entity has taken action in reliance on the authorization; or
- The authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.

### **Documentation**

Covered Entities are required to document and retain per section §165.630(j) the following:

- Signed authorizations; and
- Revocations.

### **Policies and Procedures**

Covered entities should develop policies and procedures to implement the requirements related to authorizations. A covered entity should:

- Develop a policy identifying all situations in which the covered entity would be required to request an authorization from an individual;
- Develop a procedure to request authorizations from individuals;
- Develop an authorization form with all required elements; and
- Develop a procedure for reviewing and processing all authorizations (including those requested by the covered entity or the individual). Procedure should ensure that authorizations do not have any known defects.

# Use and Disclosure – Communications with Brokers and Agents

Revision Date: 09/06/2002

## Citations

There are no direct references to the handling of communications with brokers, agents or independent producers (we will use the term ‘brokers’) in the Final Privacy Rule as Modified. In considering policies and procedures that will govern communications with brokers, one should first become familiar with the regulations governing business associates, authorizations and personal representatives. These topics are addressed in more detail within the appropriate sections of this workgroup document.

## Related Citations

- §164.504(f) – Requirements for group health plans
- §164.510(b)(2) – Uses and disclosures with the individual present
- §164.510 – Uses and disclosures for which an authorization is required
- Preamble, pg. 82508 – Discussion of permission to disclose protected health information to plan sponsor/agent
- Preamble, pg. 82522-3 – Discussion regarding personal representatives

## General Requirements

Section 160.103 of the Privacy regulations establishes the general definition of a business associate:

“... *Business associate* means, with respect to a covered entity, a person who on behalf of such covered entity... performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information...”

In order to determine its policies and procedures related to communications with brokers, a covered entity must first assess its existing broker relationship(s). Typically, brokers will be in the business of performing a function on behalf of their client who may be an employer, a health plan or a member. Brokers predominantly provide three functions within the healthcare delivery system:

- Collecting enrollment information (often including health surveys) for new or prospective business;
- Collecting payment history information and reports in order to assess the plan’s or TPA’s performance; and/or
- Acting as a liaison to resolve questions or issues related to enrollment, authorizations or claims payment.

These functions may be performed on behalf of the health plan, the employer, the individual member or a combination of the three. The covered entity must assess not only the function the broker is performing but also the party on whose behalf the broker is performing this function then develop policies that support those authorized functions.

If the broker is performing business functions on behalf of the health plan, the broker should be treated in accordance with the guidance on business associates. Any services provided and/or information disclosed

should be specifically for furthering the business purpose(s) specified in the broker's business associate agreement with the health plan.

If the broker is performing business functions on behalf of the employer, the broker should be treated in accordance with the guidance on use and disclosure – employer/plan sponsor. Any services provided and/or information disclosed should be specifically for furthering that business purpose(s) specified in the broker's service agreement with the employer and consistent with what would otherwise be provided to the employer. As discussed in 165.504 (f), the plan documents must also be revised to support this activity.

*"The plan sponsor agrees to ... 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."*  
[164.504 (f)(2)(ii)(B)]

It may also be the case where a broker would act outside of a contract for services and serve as a liaison for a member seeking resolution on a problem related to authorization, payment or access to a provider. This activity is commonplace in the support of individual insurance policies. Under the privacy regulations, however, release of information to a broker who is not a business associate of the health plan would not be allowed without special authorization from the member. In these instances, the broker should be treated in accordance with the guidance on Authorizations.

Accepting enrollment information from a broker does not, in turn, create an obligation for a health plan to provide that broker with subsequent information it collects regarding that enrollee. Once the information is passed to or collected by a covered entity (or a business associate acting on the covered entity's behalf), that entity is obligated to protect the information in compliance with applicable law.

## **Policies and Procedures**

A covered entity must bring clarity to its broker relationships by ensuring that broker service agreements and/or business associate agreements are in place and accurately reflect the services for which the broker is contracted. The covered entity must then develop policies and procedures designed to support these relationships as specified in the broker agreements. Disclosures not related to the business purposes specified in a broker's agreement or to a broker that does not hold an appropriate services agreement with the employer, health plan or member, would not be allowed. Policies, practices and data management systems must be developed around the ability to know which brokers have an agreement in place to receive information on behalf of the employer, the health plan or member.

When it is determined appropriate to disclose information to a broker, the standards of minimum necessary, permitted use and disclosure, and the right to restrict disclosures must govern that release.

# Use and Disclosure – Deceased Individuals

Revision Date: 09/06/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy preambles address the requirements regarding the protected health information (PHI) of deceased individuals and the policies and procedures required to implement the standard:

- §164.502 (f) – Uses and disclosures of protected health information: general rules – Standard: deceased individuals
- §164.502 (g)(4) – Uses and disclosures of protected health information: general rules – Standard: personal representatives – Implementation specification: deceased individuals
- §164.512 (g) – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required – Standard: uses and disclosures about decedents
- §164.512 (h) – Use and disclosures for cadaveric organ, eye or tissue donation purposes-Research on decedent’s information
- §164.512 (i) – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required – Standard: uses and disclosures for research purposes
- Preamble, pg. 82482 & 82597 – Freedom of Information Act
- Preamble, pg. 82499-500, 82534 & 82631-82634 – Deceased Individuals & Personal Representatives
- Preamble, pg. 82537 – Research and Decedents’ protected health information
- Preamble, pg. 82659 – Disclosure of decedents’ protected health information for the purpose of claiming death benefits
- Preamble, pg. 82492 – Definition of individual
- Preamble, pg. 82532 – Disclosures about decedents
- Preamble, pg. 82545 – Uses & disclosures for research

## General Requirements

The general rule requires a covered entity to protect the PHI of a deceased individual for as long as it maintains the information. The rule allows the covered entity to disclose a decedents’ PHI to coroners or medical examiners and funeral directors. The rule also permits covered entities to disclose PHI for the purpose of research as discussed in detail below. Finally, the rule also requires covered entities to treat individuals lawfully representing decedents just as they would the deceased individuals if they were alive.

## Policies and Procedures

The HIPAA Privacy Rule extends the protection of PHI about deceased individuals to remain in effect for as long as the covered entity maintains the information. Under the standard the covered entity must treat an executor, administrator, or other person who has authority to act on behalf of a deceased individual as a

personal representative with respect to PHI. In other words, the covered entity must treat the personal representative of an individual as the individual.

Except for uses and disclosures for research purposes, the covered entity must protect the PHI of a deceased individual in the same manner and to the same extent as required for the PHI of living individuals.

The HIPAA Privacy Rule allows disclosure of deceased individuals' PHI to health care providers for the purposes of treatment. If the PHI about the deceased person is relevant to the treatment of a family member, the family member's health care provider may obtain that information.

### **Permitted Disclosures**

The following disclosures of PHI about the deceased individual are allowed:

- Disclosures to coroners and medical examiners for identification of a deceased person or to determine cause of death;
- In cases where a covered entity is itself a coroner or medical examiner, the covered entity is permitted to disclose PHI for its duties as a coroner or medical examiner;
- Disclosures to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to a decedent. These disclosures may occur prior to and in reasonable anticipation of the individual's death; and
- Disclosures to personal representatives as discussed in detail in this paper under section titled "Personal Representatives".

### **Disclosures for the purpose of Research**

The use and disclosure of PHI of deceased persons for research purposes is permitted without obtaining authorization from a personal representative and absent approval by an IRB or privacy board provided that the covered entity obtains the following from the researcher:

- Representation that the use or disclosure is sought solely for research on the protected health information of decedents;
- Documentation, at the request of the covered entity, of the death of such individuals; and
- Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

### **Disclosures and the Freedom of Information Act (FOIA)**

As a general rule, PHI requested under FOIA would come within FOIA Exemption 6. The PHI of a deceased individual may require special consideration since under the Privacy Act privacy rights are extinguished at death. It is appropriate, however, to consider the privacy interests of a decedent's survivors under Exemption 6. If there are state laws that require deceased PHI be made public, covered entities should comply with those laws. Otherwise, covered entities subject to FOIA must evaluate each disclosure on a case-by-case basis.

### **Cadaveric organ, eye or tissue donation purposes**

A covered entity may use or disclose PHI 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.

# Use and Disclosure - De-identification of Protected Health Information

*Revision Date: 09/30/02*

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy preambles discuss de-identification of protected health information:

- §164.502 (d) – Uses and disclosures of protected health information – Standard: Uses and disclosures of de-identified protected health information.
- §164.514 (a) – Other requirements relating to uses and disclosures of protected health information – Standard: de-identification of protected health information.
- §164.514 (b) – Other requirements relating to uses and disclosures of protected health information – Implementation specifications: Requirements for de-identification of protected health information.
- §164.514 (c) – Implementation specification: Re-identification of information
- Preamble, pgs. 82499, 82631, 82708 – Discussion of §164.502 (d)
- Preamble, pgs. 82542, 82708 – Discussion of §164.514 (a)
- Preamble, pgs. 82542, 82708 – Discussion of §164.514 (b)
- Preamble, pgs. 82542, 82708 – Discussion of §164.514 (c)
- Modifications to the Final Rule, pgs. 53232-53234 – Discussion of de-identification
- Modifications to the Final Rule, pgs. 53234-53238 – Discussion of a limited data set
- §164.514 (e) – Limited data set

## General Requirements

Section 164.502 (d) (1) establishes the general standard for creating 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.”

Section 164.502 (d) (2) establishes requirements for uses and disclosures of de-identified information. De-identified health information is no longer considered to be individually identifiable health information and the requirements of the HIPAA Privacy Rule do not apply. However, use or disclosure of this de-identified data must not include disclosure of a code or other means of record identification designed to enable the information to be re-identified. 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.

## Policies and Procedures

The HIPAA Privacy Rule permits a covered entity to use protected health information (PHI) to create de-identified information, whether or not the de-identified information is to be used by the covered entity.

The Privacy Rule also clarifies that de-identified information created in accordance with the listed procedures (found in §164.514(a)) is not subject to the requirements of the Privacy Rule unless it is re-identified.

The preamble of the Privacy Rule discusses two ways to comply with de-identifying protected health information. The first method requires that a person with appropriate knowledge and experience apply generally accepted statistical and scientific principles and methods for rendering information not individually identifiable and certify that the information could not be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information. This person must document the method and results of the analysis.

For the second method, a covered entity is considered to have met the standard if it removes all of a list of enumerated identifiers of the individual or of relatives, employers, or household members of the individual, and if the covered entity has no actual knowledge that the information could be used alone to or in combination to identify a subject of the information. This is referred to as the safe harbor method of de-identification.

The Modifications to the Privacy Rule identified an alternative approach to de-identification that would permit a “limited data set” for research, public health and health care operations only. This limited data set would exclude obvious identifiers such as name, address, phone number, social security number, URLs, etc., but would allow additional data related to dates of care, age, city, state and zip code.

### **Statistical De-identification**

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable if this person 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. This person must document the methods and results of the analysis that justify such determination.

### **Safe Harbor Method of De-identification**

Under the “safe harbor” method of de-identification, the following identifiers of the individual or of relatives, employers, or household members of the individual, must be removed:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geo-codes, except for the initial three digits of a zip code<sup>7</sup>
- 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.
- Telephone numbers
- Fax numbers
- Electronic mail addresses

---

<sup>7</sup> The first three digits of the zip code may be used only if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people. If that is not the case, the initial three digits of a zip code for any geographic units containing 20,000 or fewer people must be changed to 000.

- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URL's)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

The covered entity must 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.

The Modifications to the Privacy Rule state that the re-identification code is not considered one of the enumerated identifiers that must be excluded under the safe harbor for de-identification. The re-identification code or other means of record identification permitted by §164.514 (c) is expressly excepted from the listed safe harbor identifiers at §164.514 (b)(2)(i)(R).

### **Policy and Procedure for a limited data set**

A covered entity may use or disclose a limited data set only for the purposes of research, public health or health care operations. A covered entity may use protected health information to create a limited data set or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- Names
- Postal address information, other than town or city, State and zip code
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers

- Web Universal Resource Locators (URL's)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

As part of the limited data set, researchers and others involved in public health studies will have access to dates of admission and discharge, as well as dates of birth and death for the individual. Birth data should only be disclosed where the researcher and covered entity agree that it is needed for the purpose of the research. The limited data set may also include the five-digit zip code or any other geographic subdivision, such as state, county, city, precinct and their equivalent geocodes, except for street address.

### **Limited data set use agreement**

A covered entity may use or disclose a limited data set if the covered entity enters into a data use agreement with the limited data set recipient. The data use agreement between the covered entity and the limited data set recipient must:

- Establish the permitted uses and disclosures of such information by the limited data set recipient. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart (164.514);
- Establish who is permitted to use or receive the limited data set; and
- Provide that the limited data set recipient will:
  - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
  - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
  - Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
  - Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
  - Not identify the information or contact the individuals.

# Use and Disclosure - Emergency Situations

Revision Date: 09/09/2002

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy preambles address the issue of use and disclosure of protected health information in emergency situations:

- §164.510 (a)(3) – Permitted uses and disclosures for facility directories during emergency situations
- §164.510(b)(3) – Limited uses and disclosures for involvement in the individual’s care and notification purposes when the individual is not present
- §164.510(b)(4) – Uses and disclosures for disaster relief purposes
- §164.512(f)(3) - Permitted disclosure: Victims of a crime
- §164.512(f)(6) - Permitted disclosure: Reporting crime in emergencies
- §164.520(c)(2) – Notice of privacy practices; specific requirements for certain health care providers
- §164.522(a)(1)(iii) - Standard: Right of an individual to request restriction of uses and disclosures; Emergency situations
- Preamble, pg. 82522 - 82523 and 82663 – Discussion of §164.510(b)
- Preamble, pg. 82531 and 82678 – Discussion of §164.512(f)
- Preamble to the Modification of the Privacy Rule, pg. 53238 – 53242 – Discussion of §164.520
- Preamble, pg. 82552 and 82726 – Discussion of §164.522(a)
- Preamble, pg. 82473, 82532-82533, 82553, 82591, 82623, 82635, 82653, 82655, 82666, 82682, 82686, 82688, 83703, 82715, 82,730, 82741, and 82795 – Additional references to use and disclosure of PHI in emergency situations

## General Requirements

The consent requirement for a health care provider to use or disclose protected health information to carry out treatment, payment or health care operations has been removed. In emergency treatment situations, §164.520(c)(2) requires the provider to provide the individual with a notice of privacy practices as soon as reasonably practicable. The health care provider is exempted in emergency situations from having to make a good faith effort to obtain the individual’s acknowledgment in such emergency situations.

Section 164.510(b)(3) allows in emergency circumstances for the covered entity to determine whether disclosure to a family member, other relative, or other person is in the best interest 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.

Section 164.512(f)(3) allows a covered entity to disclose protected health information about victims of crime to law enforcement officers if the covered entity is unable to obtain the individual’s agreement because of incapacity or other emergency circumstances.

Section 164.512(f)(6) allows a covered health care provider who is providing emergency health care, other than on the premises of the provider, to disclose protected health information to a law enforcement official if

the disclosure appears necessary to alert law enforcement to the commission and nature of a crime, location of crime, and identity, description and location of the perpetrator.

Section 164.522 (a)(1)(iii) allows a covered entity who has agreed to an individual's request for restriction of uses and disclosures to use or disclose the restricted protected health information if the individual who requested the restriction is in need of emergency treatment.

## **Policies and Procedures**

“Emergency treatment situations” are not specifically defined. The preamble suggests that the intent is to allow the provider to avoid asking permission to use or disclose protected health information when doing so would “delay treatment such that the patient's health would be jeopardized.” Any covered entity (not just a provider) may encounter situations that may be considered “emergency situations” even though they are not directly involved in treating an individual. Covered entities that anticipate encountering emergency treatment situations will need to establish policies and procedures that will:

- Establish the definition of emergency situations that are applicable to the covered entity in each of the above situations.
- Establish the type of protected health information that can be released in each of the applicable situations.
- Establish in each of the applicable situations when the notice of privacy practices will be presented to the individual and if and when provider will make a good faith effort to obtain the individual's acknowledgment.

# Use and Disclosure – To Employer/Plan Sponsor

Revision Date: 10/10/20022

## Citations

The following sections of the Final Privacy Rule as Modified and the Privacy preambles discuss requirements relating to uses and disclosures to employers and plan sponsors:

- §164.504 – Uses and disclosures: organizational requirements
- Definitions: Health Care Component, Hybrid Entity
- Standard: Health care component
- Implementation specifications
- (f)(1)Standard: requirements for group health plans
- (f)(2) Implementation specifications: requirements for plan documents
- (f)(3) Implementation specifications: uses and disclosures
- §164.514(d) – Minimum Necessary: requirements
- §164.530(k) – Administrative requirements: Group Health Plans
- Preamble, pg. 82490-1, 82495-6 – Health care operations and plan sponsors
- Preamble, pg. 82502 – Hybrid Entities
- Preamble, pg. 82507 – Group Health Plans
- Preamble, pg. 82571, 82579, 82609-10, 82628-9, 82642, 82644-8, 82723 – Related Comments
- Preamble, pg. 82772-3, 82785 – Cost analysis
- Preamble, pg. 82645, 82647 – Minimum necessary
- Preamble to the Modifications, pg 52192 – Protected Health Information

## General Requirements

Section 164.504(f) sets forth the rules and limitations for sharing protected health information (PHI) and summary health information with an employer or plan sponsor. The rule allows:

- A health plan to share summary information with a plan sponsor for purposes of obtaining premium bids from health plans or modifying, amending, or terminating the group health plan;
- That a health plan may provide access to PHI to employees of an employer or plan sponsor to carry out administrative duties of a health plan related to treatment, payment or health care operations; and
- May not disclose PHI to the plan sponsor for any employment-related actions or decisions.

Section 164.514(d) sets forth minimum necessary requirements; the preamble states that disclosures of protected health information to the plan sponsor are bound by the minimum necessary standard.

Section 164.504(a), (b) and (c) set forth the concept of a hybrid entity and calls for the “health care component” of a hybrid entity to follow the requirements described in §164.504 for a health plan. The

preamble discussion explains that no attempt is made to regulate employers; rather the strategy is to place restrictions on the flow of information from covered entities to non-covered entities. The health care component of a hybrid entity is treated as a covered entity. The final regulation further defines a hybrid entity as being a single entity that has one component that is a covered entity, has business activities of both a covered entity and non-covered entity and defines the healthcare component(s) as follows. Hybrid entities may be comprised of more than one health care component. The responsibility of each is determined as though each were a separate legal entity and by whether or not the healthcare component performs covered functions or has activities that would make one component a business associate if they were separate legal entities. [§164.504(c)(3)(iii)].

## **Policies and Procedures**

A health plan may share summary health information with an employer.

### **Procedures for a health plan to share summary information with a plan sponsor or employer**

Section 164.504(f)(1)(ii) permits sharing of summary health information with an employer provided the request is for either (a) obtaining a premium bid or (b) for modifying, amending or terminating the group health plan. The definition of summary health information is given in Section 164.504(a). This lays out the identifiers that must be removed for the information to qualify as summary information. In the preamble the point is made that this summary information may be disclosed even if it does not meet the requirements of de-identified information.

Section 164.504(f)(2)(iii) permits sharing individual enrollment and disenrollment information between health plan and sponsor without meeting the plan document amendment and other related requirements.

### **Notice of privacy practices if PHI is shared**

In Section 164.520(b)(1)(iii)(C), a covered entity is required to provide adequate notice to an individual of the uses and disclosures of protected health information that may be made by the covered entity. Section 164.504(f)(2)(ii)(J) requires a cover entity to state in its notice of privacy practices that it may share PHI with an employer or plan sponsor. In addition, the preamble that discusses summary information repeats the requirement for the notice to disclose to individuals that their protected health information may be disclosed.

**Note that a group health plan does not have to maintain notice if no PHI is created or received (only summary information or enrollment status is used) and benefits are provided solely through an insurance contract or HMO [§164.520(a)(2)(iii)].**

A health plan may share PHI with an employer or plan sponsor to carry out administrative duties. At least two procedures are indicated:

**Notice of privacy practices for protected health information:** In Section 164.520(b)(1)(iii)(C), a covered entity is required to provide adequate notice to an individual of the uses and disclosures of PHI that may be made by the covered entity. Section 164.504(f)(2)(ii)(J) requires a cover entity to include in such notice that PHI may be shared with an employer or plan sponsor as a necessary prerequisite to sharing PHI.

**Procedure for a Health Plan to share PHI with a plan sponsor or employer:** Section 164.504(f)(2)(ii) requires that a health plan receive a certification from the plan sponsor before it releases PHI to the plan sponsor. Three topics required of the plan document and the ten points that must be included in the certification are discussed in the preamble [page 82508]. The plan document must: (1) describe permitted uses of PHI, (2) specify that the plan sponsor has provided required certification, which includes the ten points below, and (3) ensure firewalls have been established. The health plan may then rely on a certification from the plan sponsor provided all 10 points are covered: (1) not to further use or disclose PHI other than as

permitted or required by plan document or as required by law, (2) ensure subcontractors agree to the same, (3) not use PHI for employment-related actions, (4) report any inconsistent use or disclosure, (5) make PHI accessible to individuals (i.e., owners), (6) allow individuals to amend their PHI, (7) provide an accounting of disclosures, (8) make practices available to the Secretary for compliance, (9) if feasible return or destroy all PHI, and (10) ensure firewalls are established. The preamble discussion on page 82508 describes the firewall requirements for employees that may be shared between a health plan and sponsor.

**Employer enrollment activity not covered by these rules**

On page 82509 the preamble notes that a plan sponsor may perform enrollment functions on behalf of its employees without meeting these conditions and without meeting the requirements of the standard transaction rule.

The Modifications to the Privacy Rule amends the definition of protected health information to exclude PHI found in employment records held by a covered entity in its role as employer. Examples of excluded information would include PHI documented for sick leave or workman's compensation.

# Use and Disclosure - Marketing and Fundraising

Revision Date: 10/20/02

## Citations

Five sections of the of the Final Privacy Rule as Modified and the Privacy preambles address the uses and disclosure of protected health information (PHI) for marketing and fundraising:

- §164.501 – Definitions – Health care operations, Marketing
- §164.508(a) – Uses and disclosures for which authorization is required
- §164.508(b) – Implementation specifications for authorizations
- §164.514(f) – Standard: Uses and disclosures for fundraising
- Preamble, pp. 82493-4 – Discussion of definition of marketing
- Preamble, pp. 82545-6 and 82716 – Discussion of marketing
- Preamble, pp. 82546 and 82718 – Discussion of fundraising
- Preamble, pp. 82489-91 – Discussion of health care operations
- Preamble, pp. 82513-6 and 82651 – Discussion of uses and disclosures requiring an authorization
- Preamble to the Modifications, pp. 53813-53190 – Modifications to Marketing

## General Requirements

The August 14, 2002 Privacy Modifications provides significant clarification while simplifying the requirements regarding allowable uses and disclosures for the purpose of marketing. In general, any use or disclosure of PHI for marketing purposes requires authorization. When seeking clarification of what activities are considered marketing, one should review the definition of marketing. The Privacy Modifications removed Section 164.514(e), which in the original rule provided clarification and limitations on marketing, and replaced it with a description of the permitted uses and disclosures for a limited data set under a data use agreement. While the section number is the same, the description of the limited data set should not be construed to be related to marketing. It is important to understand that the limited data set is not fully de-identified and is, therefore, considered protected health information and subject to all restrictions applicable to protected health information.

In addition, the August 14, 2002 Privacy Modifications removed any reference to the inclusion of limited marketing activities under health care operations. In certain circumstances, defined in §164.514(f), fundraising activities may still be allowable and are included in the definition of health care operations.

### **§164.501 – Definitions – Marketing**

The definition of marketing includes any communication that encourages the recipient to purchase or use a product or service. Any reference to the intent of the communication has been removed, and the judgment of whether or not a communication is or is not marketing relies solely on the content of the document itself. The definition also lists those exceptions to communications of this nature that do not constitute marketing.

### **§164.508 (a) (3) – Uses and disclosures for which authorization is required**

This section reinforces limits on the use and disclosure of protected health information for marketing without authorization. Furthermore, it clarifies that an authorization for marketing activities must disclose any direct or indirect remuneration resulting from the activity. The rule provides two exceptions to the rules on marketing:

- Any to face-to-face communication made by a covered entity to an individual; or
- A promotional gift of nominal value provided by the covered entity.

#### **§164.514 (f) – Standard: Uses and disclosure for fundraising**

This section states that a covered entity can use and disclose to a business associate or “institutionally related foundation” limited protected health information if certain requirements are met. No modifications were made to this section in the August 14, 2002 rule.

### **Policies and Procedures**

The Privacy Modifications added more functionality to the term “health care operations” so that it “includes general administrative and business functions necessary for the covered entity to remain a viable business.” Protected health information can be used without an authorization from an individual for activities that are considered to be health care operations.

In addition, the Privacy Modifications, section §164.501, defines marketing as

(1) A communication about a product or service with the purpose to encourage recipients of the communication to purchase or use the product or service unless the communication is made:

(i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(ii) For the treatment of the individual; or

(iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Policies and procedures related to member or patient communications must differentiate between activities for health care operations and marketing and strictly limit uses and disclosures for marketing. When considering whether an activity is health care operations or marketing, rely only on the communication itself, not the underlying intent that is not known to the recipient. Any communications or activities that meet the definition of marketing require an authorization. Work flows and policies must support an individual’s right to deny authorization or terminate an existing authorization and not receive future marketing communications.

Policies and procedures governing fundraising activities should seek to control information flow to the foundation or other agencies performing fundraising activities in compliance with §164.514(f). In addition, an entity must ensure that any fundraising activity is disclosed in its Notice of Privacy Practices. Work flows and policies must support the individual’s right to restrict uses or disclosure related to fundraising, to opt-out

of receiving further fundraising communications, and to provide or deny authorization for fundraising activities not previously disclosed in the Notice of Privacy Practices.

### **Implementation specifications for Authorizations**

When a marketing or fundraising communication requires an authorization, section §164.508 describes how an authorization should be implemented. Of interest to marketing and fundraising is the description of acceptable and non-acceptable compound authorizations. Marketing and fundraising are considered to be an acceptable combination for a compound authorization. When implementing this standard, the use of protected health information to create the mailing list necessary to obtain an authorization does not require an authorization.

Because of the need to obtain authorization for all marketing activities, those provisions allowing individuals to restrict or opt-out of marketing activities becomes unnecessary and has been deleted in the final rule. If an individual wishes to stop receiving marketing communications from an entity, they need only retract their original authorization. As with other uses, a covered entity may make treatment or health plan coverage decisions based upon receipt of an authorization.

When considering the implementation of standing authorizations for ongoing activities such as marketing and fundraising, one must closely review state statutes for authorization requirements or the use of health information for marketing or fundraising activities.

Lastly, disclosure of PHI to a business associate for marketing or fundraising communications is acceptable if that business associate normally performs that service. In other words, if you normally engage the services of a marketing firm for your marketing campaigns, you may continue doing so as long as the above criteria, as well as the minimum necessary standard, applicable to the communication are met.

# Uses and Disclosure – Not Requiring an Authorization or Opportunity for the Individual to Agree or Object

Revision Date: 10/10/2002

## Citations

The following citations from the Final Privacy Rule as Modified and the Privacy preambles discuss uses and disclosures for which an authorization or an opportunity to agree or object is not required.

- §164.501 – Definitions
- §164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required
- 12/28/2000 Preamble, 65 Fed. Reg. 82,524-26, 82,528-29, 82,532, 82,534,82,539-43, 82,668-82-672, 82,688-89,82,704-08– Uses and disclosures for which an authorization or opportunity to agree or object is not required

## Related Citations

See the following Sections on Use and Disclosure in this Privacy Policies and Procedures resource document for other topics covered under Section 164.512 of the Final HIPAA Privacy Rule as Modified:

- Uses and Disclosures – Required by Law
- Uses and Disclosures – Research Activities
- Uses and Disclosures – Deceased Individuals

## General Requirements

Section 164.512 of the Final Privacy Rule as Modified describes a variety of permitted uses and disclosures that a covered entity may make without an authorization from the individual or allowing the individual an opportunity to object. This section describes several of these special situations that are not elsewhere addressed in this resource document.

### Public health activities

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

A public health authority that is authorized by law to collect or receive PHI for the purpose of preventing or controlling disease, injury, or disability, including, 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;

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

A person subject to the Food and Drug Administration's (FDA) jurisdiction concerning an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include: (A) to collect or report adverse events (or similar activities 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; (B) to track FDA-regulated products; (C) to enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or (D) to conduct post marketing surveillance;

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

An employer, about an individual who is a member of the employer's workforce, if all of the following conditions are met: (A) the covered entity is a covered health care provider who is a member of such employer's workforce or who provides health care to the individual at the employer's request: (i) to conduct an evaluation relating to medical surveillance of the workplace; or (ii) to evaluate whether the individual has a work-related illness or injury; (B) the disclosed PHI 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; and (D) the covered health care provider provides written notice to the individual that PHI 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 employer's work site, by posting the notice in a prominent place at the location where the health care is provided.

*Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use PHI for the purposes described in the permitted disclosures section above.

### **Health oversight activities**

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

*Permitted disclosures.* Subject to the exception identified below, a covered entity may disclose PHI 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: (A) the health care system; (B) Government benefit programs for which health information is relevant to beneficiary eligibility; (C) entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or (D) entities subject to civil rights laws for which health information is necessary for determining compliance.

*Exception:* PHI generally may not be disclosed in connection with an investigation or other activity in which (A) the individual is the subject of the investigation or activity and (B) 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.

*Caveat -- Joint activities or investigations.* 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 which disclosure is permitted.

*Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use PHI for the purposes described in the Permitted Disclosures section above.

### **Cadaveric organ, eye or tissue donation purposes**

A covered entity may use or disclose PHI 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.

### **Specialized government functions: military and veterans activities**

**Armed Forces personnel.** A covered entity may use and disclose the PHI of 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 in the Federal Register a notice containing the following information: (A) appropriate military command authorities; and (B) the purposes for which the PHI may be used or disclosed.

**Separation or discharge from military service.** A covered entity that is a component of the U.S. Defense Department or the U.S. Transportation Department may disclose to the U.S. Veterans Affairs Department (DVA) the PHI of an Armed Forces member upon that individual's separation or discharge from military service for the purpose of a DVA determination of the individual's eligibility for or entitlement to DVA benefits.

**Veterans.** A covered entity that is a DVA component may use and disclose PHI to DVA components that determine eligibility for or entitlement to, or that provide, DVA benefits.

**Foreign military personnel.** A covered entity may use and disclose the PHI of 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 Federal Register notice.

### **Specialized government functions: National security and intelligence activities**

A covered entity may disclose PHI to authorized federal officials for the conduct of lawful national security and intelligence activities.

### **Specialized government functions: Protective services for the President and others**

A covered entity may disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by federal law, or to foreign heads of state or other persons authorized by federal law, or to for the conduct of investigations authorized by 18 U.S.C. §§871 and 879.

### **Specialized government functions: State Department**

A covered entity that is a State Department component may use PHI to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the State Department officials who need access to such information for the following purposes: (A) for a required

security clearance; (B) as necessary to determine worldwide availability or availability for mandatory service abroad; or (C) for a family to accompany a Foreign Service member abroad.

### **Correctional institutions and related law enforcement custodial situations**

Permitted disclosures. A covered entity may disclose PHI to a correctional institution or a law enforcement official having lawful custody of an inmate or other person who is the subject of the PHI if the correctional institution or such law enforcement official represents that such PHI 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.

Permitted uses. A covered entity that is a correctional institution may use PHI of individuals who are inmates for any purpose for which such PHI may be disclosed.

Limitation. These rules do not apply 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 benefit**

A health plan that is a government program providing public benefits may disclose PHI 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.

A covered entity that is a government agency administering a government program providing public benefits may disclose PHI 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 PHI disclosure is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

### **Workers' compensation**

A covered entity may disclose PHI 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.

## **Policies and Procedures**

Covered entities are required to establish, maintain, and train workforce members on policies and procedures in all the areas listed above to the extent that such special situations may be applicable to the covered entity.

# Use and Disclosure - Minimum Necessary

Revision Date: 09/30/2002

## Citations

Three sections of the Final Privacy Rule as Modified and the Privacy preambles address the minimum necessary standard and the policies and procedures required to implement the standard:

- §164.502(b) – Uses and disclosures of protected health information: General rules – Standard: Minimum necessary
- §164.514(d) – Other requirements relating to uses and disclosures of protected health information: Standard: Minimum necessary requirements
- Preamble, pg. 82499, 82631, 82712 – 82716, and 82726 – Discussion of comments on minimum necessary
- Preamble, pg. 82543 – 45 – Discussion of minimum necessary
- Modifications to the Final Rule, pg. 53195-53198

## General Requirements

In §164.502(b), the HIPAA Privacy Rule establishes the general standard for minimum necessary:

*“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.”*

This section also explains the situations in which minimum necessary does **NOT** apply:

- Disclosures or requests by a health care provider for treatment;
- Uses or disclosures made to the individual or the individual’s personal representative,
- Uses or disclosures made to an individual in an accounting of disclosures (164.528);
- Uses or disclosures of an individual’s designated medical record when a request for access has been made by the individual (164.524);
- Uses or disclosures made pursuant to an authorization under §164.508;
- Disclosures made to the Secretary;
- Uses or disclosures required by law as described in §164.512(a); and
- Uses or disclosures required to comply with the HIPAA Privacy Rule.

The steps a covered entity must take to ensure the implementation of the minimum necessary standard are outlined in §164.514 (d)(1-5). A covered entity must “reasonably ensure” that the minimum necessary standard and its requirements are implemented in regard to use, disclosure and requests for protected health information.

The covered entity may rely on a request for disclosure as being for the minimum necessary amount of information if:

- The disclosure is to a public official and is permitted under §164.512 and the public official represents that the request is for the minimum necessary information;
- The request is from another covered entity;
- The request is from a professional in its own workforce or from a business associate in order to provide a professional service to the covered entity and the professional represents that the request is for the minimum necessary information; or

The requestor provides documentation or representations that meet the requirements for use and disclosure of protected health information for research purposes as explained in §164.512(i).

The Modifications to the Final Rule emphasize that a covered entity may reasonably rely on a researcher's documentation or on the representation of an IRB or privacy board regarding the minimum necessary information requested for research purposes.

HHS also notes that disclosures to financial institutions for processing payment transactions are subject to minimum necessary restrictions. A covered entity is allowed to reasonably rely on a financial institution's request for information. However, the covered entity must make its own assessment of the minimum necessary information necessary for the financial institutions purpose.

## **Policies and Procedures**

The preamble to the December 2000 publication of the Privacy Rule discusses in detail the requirements in §164.514(d) for implementing the minimum necessary standard. It states that a covered entity must develop policies and procedures to implement the minimum necessary standard. These policies and procedures apply to all uses and to many disclosures and requests for disclosures from other covered entities. Implementing these policies and procedures will eliminate the need to make minimum necessary decisions about every separate use, disclosure or request.

The language in the preamble creates a duty on the part of covered entities to identify situations where they may need to use professional judgment when determining how to apply the minimum necessary standard. Policies and procedures should address this duty and outline criteria which can be used to determine the reasonableness of a disclosure request.

In general terms, these policies and procedures must accomplish the following:

- Restrict access and use based on specific roles of members of the covered entity's workforce;
- Establish criteria to limit routine disclosures to the minimum necessary to achieve the purpose of the disclosure; and

Limit requests to other covered entities to what is reasonably necessary for the particular use or disclosure.

*Note: The preamble again emphasizes that disclosures or requests by a health care provider for treatment purposes are **NOT** subject to the minimum necessary standard.*

### **Policies and procedures for uses by the covered entity's workforce**

For *uses* of protected health information, the covered entity must:

- Identify the persons or groups of persons who need access to protected health information to carry out their job function;

- Identify the type of protected health information to which each person or group needs access as well as the conditions under which they need the access; and
- Make reasonable efforts to limit the access of its staff to only the information appropriate to their job requirements.

### **Policies and Procedures for Disclosures of PHI**

For *disclosures* of protected health information by its own workforce, the rule distinguishes between routine, recurring disclosures and all other disclosures.

For routine, recurring disclosures, the covered entity must implement policies and procedure that identify:

- The types of protected health information to be disclosed;
- The types of persons who would receive the protected health information;
- The conditions that would apply to such access; and

Standards for disclosures to routinely hired types of business associates (e.g., for medical transcription).

Since there may be considerable variation in the disclosures within the same type of disclosure, the policies should address the norm for the type of disclosure.

For non-routine disclosures, the covered entity must:

- Develop reasonable criteria to limit the amount of information disclosed to the minimum necessary to accomplish the purpose of the disclosure; and
- Use these criteria to review these disclosures on an *individual basis*.

### **Policies and Procedures for Requests for PHI**

When *requesting* protected health information from other covered entities, a covered entity must limit its request to that which is “reasonably necessary” to accomplish the purpose of the request. Again, the rule distinguishes between routine, recurring requests and all other requests.

For routine, recurring requests, the covered entity must implement policies and procedures that:

- Describe what information is reasonably necessary for the purpose of the request; and
- Limit the request for protected health information to that information.

These policies and procedures may be standard protocols that are used for these requests.

For all other requests, the covered entity requesting the information must review the request on an individual basis to determine that the protected health information requested is limited to the information reasonably necessary to accomplish the purpose of the request.

While a covered entity may request information that is later disclosed to a third party (e.g., for quality assessment purposes), the request must meet the minimum necessary requirement.

### **Policies and Procedures Regarding the Entire Medical Record**

In regard to requests for an entire medical record, the rule specifically limits the use, disclosure or request for an entire medical record to instances where the entire medical record is specifically justified as reasonably necessary.

Covered entities must have policies and procedures that control when they request or disclose the entire medical record. The Modifications to the HIPAA Privacy Rule emphasize that minimum necessary principles

are supposed to be consistent with, not in opposition to, professional judgment, as reflected in each covered entity's policies and procedures. These policies must specifically justify why the entire medical record is required. The preamble issues a stern warning that disclosure of the entire medical record without such documentation is a "presumptive violation" of the rule.

Note: The preamble emphasizes that the covered entity's policies and procedures may allow access to the entire medical record to providers involved in treatment of an individual.

# Uses and Disclosures – Permitted Under the Privacy Rule

*Revision Date: 10/101/2002*

## Citations

The following citations from the Final Privacy Rule as Modified and the Privacy preambles discuss permissible uses and disclosures.

- §164.501 – Definitions
- §164.502 – General Rules for Uses and Disclosures of Protected Health Information
- §164.504 – Uses and disclosures: organizational requirements.
- §164.506 – Uses and disclosures to carry out treatment, payment, or health care operations
- §164.508 – Uses and disclosures for which an authorization is required
- § 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object
- §164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required
- §164.524 – Access of individuals to protected health information
- §164.528 – Accounting of disclosures of protected health information
- 12/28/00 Preamble, pg. 82,498 – 82,502 – General rules for uses and disclosures of protected health information

## Related Citations

See the following Sections on Use and Disclosure in this Privacy Policies and Procedures resource document for more detailed consideration of permissible uses and disclosures :

- Uses and Disclosures – Communications with Brokers and Agents
- Uses and Disclosures – Consent (Appendix C)
- Uses and Disclosures – Deceased Individuals
- Uses and Disclosures – to Employer/Plan Sponsors
- Uses and Disclosures – Marketing and Fundraising
- Uses and Disclosures – Requiring an Opportunity for the Individual to Agree or to Object
- Uses and Disclosures – Required by Law
- Uses and Disclosures – Research Activities
- Uses and Disclosures – Underwriting and Related Purposes

## General Requirements

The Final HIPAA Privacy Rule as Modified controls the use and disclosure of protected health information (PHI) by covered entities. Generally, covered entities may not use or disclose PHI except in ways that are specifically allowed by the Final HIPAA Privacy Rule as Modified, including certain treatment, payment and healthcare operation functions. All other uses and disclosures are prohibited and barriers must be established by covered entities to prevent any use and disclosure other than those permitted.

*Use* of PHI includes anything done with the information *inside* the covered entity (i.e., “sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information,” 45 CFR §164.501).

*Disclosure* of PHI means anything done with the information *outside* of the covered entity (i.e., “release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information,” 45 CFR §164.501)

Covered entities are expressly allowed to use and disclose PHI for treatment, payment, and health care operations. The uses and disclosures for treatment are generally very broad, allowing information to be exchanged between any number of entities that deliver, coordinate, manage, or are in any way involved with patient care.

In order to use or disclose an individual’s PHI, a covered entity must follow proper procedures, which may include written permission (in the form of an authorization). In addition, the individual must be given a Notice of Privacy Practices that says how PHI will be used.

Use and disclosure of PHI is typically restricted to specific persons, and kinds of jobs, which are authorized to access, use, disclose, and request PHI. There are also restrictions on the kind of PHI that authorized persons may access, and the conditions under which they may access the information. Each covered entity should have its own policies and procedures that determine proper use and disclosure of PHI.

In section 164.502 (a), the Final HIPAA Privacy Rule as Modified defines the general standard for uses and disclosures of PHI. As mentioned above, covered entities may use and disclose PHI only as permitted by the rule. Following are the general rules for required and permitted uses and disclosures under the Final HIPAA Privacy Rule as Modified, all other disclosures will generally require an authorization:

Required disclosures:

- To an individual for their own PHI if they ask to see or copy the information or if they request an “Accounting of Disclosures.”
- To the Department of Health and Human Services for purposes of determining the covered entity’s compliance with the Privacy Rules.

Permitted uses and disclosures:<sup>8</sup>

- For treatment payment or health care operations
- Incident to a use or disclosure otherwise permitted.

Permitted uses and disclosures requiring a verbal agreement and opportunity to agree or object:

- Facility directories
- Persons assisting in the individual's care

---

<sup>8</sup> The Privacy Rule Modifications published 8/14/02 eliminate the requirement on health care providers to seek consent prior to use of protected health information for treatment, payment and healthcare operations. Providers may seek consent if they wish and state regulations may require that the provider do so.

Permitted uses and disclosures for which an authorization or opportunity to agree or object are not required:

- Required by law
- Public health activities
- Victims of abuse, neglect or domestic violence
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement
- Victims of a crime
- Decedents (coroners, medical examiners, funeral directors)
- Cadaveric organ, eye or tissue donation
- Research purposes
- Avert a serious threat to health and safety
- Specialized government functions
- Workers compensation

#### **Related Privacy Rule Requirements.**

Following are additional Privacy Rule requirements pertaining to permitted use and disclosures that are covered more completely in other areas of this document:

- **Minimum Necessary:** “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 the protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.” (45 CFR § 164.502(b) and §164.514(d)).
- **Whistleblowers:** “The 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” in good faith to a health oversight agency or attorney(45 CFR § 164.502(j)(1)).
- **Victims of crime:** “[A] covered entity is not considered to have violated the requirements of this subpart [minimum necessary provision], if a member of its workforce who is a 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 under § 164.512(f)(2)(i). (45 CFR § 164.502(j)(2)).
- **Personal Representative:** If 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... with respect to protected health information relevant to such personal representation” (45 CFR § 164.502(g)(1)). Personal representatives have the same rights as the individual.
- **Unemancipated Minors:** A person who is under the age of majority as defined by applicable state law and who has not exercised any right to emancipation under such state law. “If under applicable law, a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an \* \* \* an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative.” (45 CFR § 164.502(g)(3)) (The Final Privacy Rule as Modified obligates the covered entity to adhere to state law which may prohibit, allow or require disclosures to parents,

guardians, and persons in loco parentis who are not serving as the personal representative in a particular situation.)

- **Deceased Persons:** “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...” (45 CFR § 164.502(g)(4)).
- **De-Identification:** “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) A covered entity may determine that health information is not individually identifiable, 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 ...or (2)(i)...identifiers [as listed in the privacy rule] of the individual or of relatives, employers, or household members of the individual are removed.” (45 CFR § 164.514(a))
- **Marketing :** Covered entities are not permitted to use or disclose PHI to market products or services that are not health-related without the express authorization of the individual; in addition, Covered entities are prohibited from selling lists of patients or enrollees to third parties without authorization. Excluded from “marketing” definition are certain health-related communications: that describe health related products or services provided by the health plan, or communications for the treatment of the individual or for case management or care coordination. and do not require authorization
- **Underwriting:** The Final Privacy Rule as Modified requires a health plan to obtain an authorization to use PHI for underwriting and risk determination for a new applicant. It also allows the plan to condition enrollment on the authorization, except enrollment may not be conditioned on psychotherapy notes. “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.” (45 CFR § 164.514(g)).
- **Verification:** Covered entities must verify the identity of any person requesting PHI. Where the identity/authority of a requestor is not known, the covered entity must also verify the authority of such person to have access to the PHI. Documentation, statements, or representations, whether oral or written, that are required as a condition of disclosure must be obtained from the person requesting PHI. There are exceptions for uses and disclosures for facility directories (where an opportunity exists for person to agree or object to disclosures), and for uses and disclosures where a person is involved in the individual’s care, and for certain other notification purposes. (45 CFR § 164.514(h))
- **Victims of Abuse, Neglect, Domestic Violence and Crime:** An exception exists for PHI disclosures by workforce members who are victims of crime, abuse, neglect, or domestic violence. (45 C.F.R. § 164.512(f)(3))

## Policies and Procedures

Covered entities are required to establish, maintain, and train workforce members on policies and procedures in all the areas listed here. Guidance on policies and procedures for each of the individual topics may be found in parts of this document that address the specific topics.

# Use and Disclosure - Personal Representatives

Revision Date: 09/06/2002

## Citations

Four sections of the HIPAA Privacy Rule and the preamble and one section of the Modification to the HIPAA Privacy Rule address the subject of personal representatives and the policies and procedures required to implement the standard:

- §164.502(g) – Uses and disclosures of protected health information: general rules – Standard: personal representatives
- §164.524 – Access of individuals to protected health information
- §164.528 – Accounting of disclosures of protected health information
- §164.510(b) – Uses and disclosures requiring an opportunity for the individual to agree or to object – Standard: uses and disclosures for involvement in the individual’s care and notification purposes
- §164.512(c)(2)(ii) – Disclosures about victims of abuse, neglect or domestic violence
- Preamble, pg. 82500 and 82633 – Discussion of §164.502(g)
- Preamble, pg. 82544 and 82731 – Discussion of §164.524
- Preamble, pg. 82599 and 82739 – Discussion of §164.528
- Preamble, pg. 82522 and 82633 – Discussion of §164.510(b)
- Preamble, pg. 82528 – Discussion of §164.512(c)
- Modification to the HIPAA Privacy Rule, §164.502(g) – Uses and disclosures of protected health information: general rules – Standard: Personal representatives

## General Requirements

Covered entities must, with two exceptions defined in the final HIPAA Privacy Rule, treat a personal representative as the individual. The final HIPAA Privacy Rule gives specific guidelines for:

- Personal representatives;
- Adults and emancipated minors;
- Unemancipated minors;
- Deceased individuals; and
- Abuse, neglect, and endangerment situations.

## Policies and Procedures

The preamble indicates the definition of “individual” has changed from the NPRM. In the final HIPAA Privacy Rule, the definition of “individual” is limited to the subject of the protected health information. This includes unemancipated minors and other individuals who may lack capacity to act on their own behalf.

In addition, the preamble notes that disclosure of protected health information to a personal representative is mandatory under this rule only if disclosure to the individual is mandatory. Disclosure to the individual is mandatory only under §164.524 and §164.528.

The preamble also states that the final rule continues to allow covered entities to use their discretion to disclose certain protected health information to family members, relatives, close friends, and other persons assisting in the care of an individual, in accordance with §164.510(b).

### **Policy and Procedure for Personal Representatives**

The final rule states that a covered entity must, except as provided under the unemancipated minors and the abuse, neglect, endangerment situations paragraphs below, treat a personal representative as the individual for purposes of this subchapter.

### **Policy and Procedure for 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.

### **Policy and Procedure for 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.

However, if 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, then, 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.

Per the Modification to the HIPAA Privacy Rule, notwithstanding the above, a covered entity:

- May disclose protected health information to a parent, guardian, or other person acting *in loco parentis* if applicable State law (including case law) permits such disclosure.
- May NOT disclose protected health information to a parent, guardian, or other person acting *in loco parentis* if applicable State law (including case law) prohibits such disclosure.
- May provide or deny access to protected health information to a parent, guardian, or other person acting *in loco parentis* that is not the personal representative as defined in this section if State law does not explicitly require the minor's assent to sharing the information with a personal representative, subject to the licensed healthcare professional's judgement that the disclosure is in the best interest of the individual.

### **Policy and Procedure for 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.

### **Policy and Procedure for 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 the covered entity has a reasonable belief that:

- The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
- Treating such person as the personal representative could endanger the individual; and
- In the exercise of professional judgment, the covered entity decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

### **Workgroup Concern**

Note: The above information addresses uses and disclosures involving personal representatives as described in the regulation. It does not, however, treat the subject matter of defining a personal representative nor does it define the terms through which one may become a personal representative. This matter is referenced only indirectly in §164.502(g)(2): "If under applicable law a person has authority to act on behalf of an individual." A thorough treatment of this subject matter, therefore, requires research into any applicable state laws governing the release of protected health information, guardianship and the delegation of healthcare decision making through a personal representative or equivalent relationship. Thus, it is important for covered entities to review, per the State law applicable to them, what constitutes a personal representative and what are the requirements that will permit verification of such relationship. 9

---

9 A tabular survey of State laws concerning minor consent to health care is available from the Alan Guttmacher Institute's web site at <http://www.guttmacher.org/pubs/journals/gr030404.pdf>.

# Use and Disclosure - Required by Law

Revision Date: 09/07/2002

## Citations

The following sections of the Privacy rule and its preamble address the issue of uses and disclosures required by law.

- §164.501 – Definitions - Required by law
- §164.512 (a) (c) (e) (f) – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required
- §164.502(b)(2)(iv) – May use or disclose PHI to the extent that such use or disclosure complies with and is limited to the relevant requirements of such law.
- §164.512(d)(2) – Exception to health oversight activities
- §164.514(d)(3)(iii)(A) – Implementation specification: Minimum necessary disclosures of protected health information
- §164.514(h)(1) – Verification requirements
- §164.528(a)(2) – Accounting of disclosures of protected health information
- Preamble, pg. 82524 – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required
- Preamble, pg. 82493 – Definition – Law Enforcement Official
- Comments, pg. 82666 – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required
- Preamble, pg. 82528 –82529 – Overlap between Law Enforcement and Oversight
- Preamble, pg. 82531 – Disclosure for Law Enforcement Purposes
- Comments, pg. 82678 – Disclosures for Law Enforcement Purposes
- Comments, pg. 82681 – 82686 – Disclosures to Law Enforcement

## General Requirements

Discussion in the Preamble (page 82525) reminds us that the only disclosures of protected health information compelled by the rule are disclosures to an individual (or the personal representative of an individual), or to the Secretary for enforcement purposes. The rule permits uses and disclosures as required by other laws and will not sanction covered entities for making such uses and disclosures. The general rule is that covered entities are permitted to use and disclose protected health information without an individual's consent, authorization or opportunity to agree or object as required by law as long as the use and disclosure complies with, and is limited to, the relevant requirements of such law.

The definition of “required by law” refers to a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. The definition offers an illustrative, though not exhaustive, list of circumstances of permitted uses and disclosures that includes the following:

- Court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information;
- A civil or an authorized investigative demand;
- Medicare conditions of participation with respect to health care providers participating in the program; and
- Statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- The rule outlines three uses and disclosures required by law for which additional requirements must be met:
  - Disclosures about victims of abuse, neglect or domestic violence;
  - Disclosures for judicial and administrative proceedings; and
  - Disclosures for law enforcement purposes.

**Disclosures about victims of abuse, neglect or domestic violence §164.512 (c)**

Covered entities may disclose protected health information for this purpose, if required by law, to an appropriate government authority if:

- The individual agrees with the disclosure;
- The disclosure is expressly authorized by statute/regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against individual and is necessary for an imminent enforcement activity; and
- The individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect, and violence.

**Disclosures for judicial and administrative proceedings §164.512 (e)**

Covered entities may disclose protected health information for a judicial or administrative proceeding in response to:

- An order of a court or administrative tribunal (disclosure must be limited to protected health information expressly authorized by the order); and
- A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, if
  - The covered entity is satisfactorily assured<sup>10</sup> that individual has been given notice of the request, or
  - The covered entity is satisfactorily assured<sup>11</sup> that party seeking information has made reasonable efforts to receive a qualified protective order.<sup>12</sup>

---

<sup>10</sup>“Satisfactory assurance” is achieved by the following: party seeking information provides a written statement to covered entity with documentation demonstrating individual has been contacted, or attempted to be contacted; the notice to the individual was descriptive enough to permit the individual to raise an objection to the proceeding; and the time for objections has elapsed and no objections were filed or filed objections were resolved and disclosures are consistent with resolution. Alternatively, it is acceptable for the covered entity to make an effort to notify the individual in accordance with the steps above.

Section §164.512(e)(2) further clarifies that requirements for use or disclosure for a judicial or administrative proceeding do not supersede other requirements of this section. The more permissive or restrictive requirements of other sections take precedence.

### **§164.514(h)(1 (f))**

Covered entities may disclose protected health information for law enforcement purposes listed below to a law enforcement official if meeting the following conditions:

Pursuant to process and as otherwise required by law [§164.512 (f) (1)]: Except as required by law for reports of child abuse or neglect or disclosures about victims of abuse, neglect or domestic violence, a covered entity may disclose protected health information pursuant to a process and as otherwise required by law if the information sought is relevant and material, the request is specific and limited to amount reasonably necessary, and it is not possible to use de-identified information.

Limited information for identification and location purposes [§164.512 (f) (2)]: A covered entity may disclose protected health information to identify or locate a suspect, fugitive, material witness or missing person. Disclosure can include a specific list of items (name, address, date and place of birth, social security number, ABO blood type and RH factor, type of injury, date and time of treatment, date and time of death and other distinguishing physical characteristics). Except as permitted by previous list, certain information cannot be disclosed, including DNA or DNA analysis, dental records, or information about body fluids or tissue.

Victims of a crime [§164.512 (f) (3)]: A covered entity may disclose protected health information about a suspected victim of a crime if the individual agrees to disclosure or without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in best interest of individual, as determined by professional judgment of covered entity.

Decedents [§164.512 (f) (4)]: A covered entity may disclose protected health information about a deceased individual if the covered entity has suspicion that death resulted from criminal conduct.

Crime on premises [§164.512 (f) (5)]: A covered entity may disclose protected health information that the covered entity judges to constitute evidence of criminal conduct that occurred on covered entity's premises.

Reporting crime in emergencies [§164.512 (f) (6)]: A covered health care provider providing emergency health care, other than such emergency on the premises of the provider, may disclose protected health information to alert law enforcement regarding the nature of a crime, and information about the perpetrator of such crime. This permissible disclosure supercedes requirements relating to victims of abuse, neglect or domestic violence.

### **Accounting of disclosures of protected health information §164.528**

---

<sup>11</sup> "Satisfactory assurance" is achieved by the following: party seeking information provides a written statement to covered entity with documentation demonstrating that the parties to the dispute have agreed to and presented a qualified protective order to the court or administrative tribunal; or the party seeking protected health information has requested a qualified protective order from such court or administrative tribunal.

<sup>12</sup>"Qualified protective order" is an order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- Prohibits parties from disclosing PHI for any purpose other than the proceedings for which the information was requested; and
- Requires return of PHI to covered entity, or destruction of all copies at the end of the proceeding.

It is acceptable for the covered entity to seek the qualified protective order in accordance with the requirements outlined above.

- A covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official if the agency or law official provides the entity with a written statement as to why the accounting would impede the investigation and specify the length of time the suspension is required.
- A covered entity may accept an oral notification if the covered entity documents:
- The identity of the agency or official
- Temporarily suspend the right to disclosures to no longer than 30 days unless a written statement is submitted during that time period.

**Additional requirements related to uses and disclosures required by law:**

- As stated in §164.502(b)(2)(iv), the uses and disclosures described in the §164.512(a) are limited to what is minimum necessary. The section covering minimum necessary requirements goes on to state that covered entities can rely that the public official making the request for information is requesting the minimum amount necessary for the stated purpose.
- Disclosures for health oversight and required by law are very narrowly defined. The distinguishing activities of the oversight agency do not include an investigation or activity in which the individual is the subject of the investigation or activity nor is directly related in health care fraud.

The verification provisions (authenticating the identity of an individual requesting protected health information and his/her authority to have access to such information) outlined in 164.514(h) apply to disclosures required by law (see Privacy Policies and Procedures: Verification of Identity of those Requesting Protected Health Information).

**Policies and Procedures**

Covered entities will need to develop policies and procedures reflecting the administrative handling of and responding to requests for disclosures required by law. Components of policies and procedures should:

- Ensure that the use or disclosure is, in fact, required by another law;
- Ensure that the use or disclosure meets the requirements of the law and is limited to what is relevant to the law;
- Specifically address the types of disclosures required by law for which additional requirements apply;
- Provide a process for applying professional judgment regarding waiving individual notification, such as for victims of abuse, neglect or domestic violence;
- Allow reliance on the public official that a request is for minimum amount of protected health information necessary for purpose; and
- Provide a process for authenticating individual or entity requesting information.

# Uses and Disclosures - Requiring an Opportunity for the Individual to Agree or to Object

*Revision Date: 0906//2002*

## Citations

One section of the HIPAA Privacy Rule and preamble addresses the uses and disclosures of protected health information requiring opportunity for the individual to agree or to object. It is for:

- §164.510(a) – Use and disclosure for facility directories - Standard
- §164.510(b)(1-3) – Uses and disclosures for involvement in the individual’s care and notification purposes – Standard
- §164.510(b)(4) – Uses and disclosures for disaster relief purposes – Standard
- Preamble, pg. 82521-4 and 82662-6 – Discussion of uses and disclosures requiring an opportunity to agree or object
- Preamble, pg. 82552 – Discussion of requesting a restriction and impact on objecting or agreeing to disclosures.

## General Requirements

§164.510 allows, but does not require, covered entities to use or disclose protected health information:

- For health care institutions, for facility directories; and
- To family members, close friends, or other persons assisting in an individual’s care,
- To government agencies and disaster relief organizations conducting disaster relief activities.

The modified rule no longer requires a consent or authorization, only that the individual is informed in advance of the use or disclosure and has an opportunity to agree, prohibit or restrict the use or disclosure.

This section addresses situations in which the interaction between the covered entity and the individual is relatively informal. Agreements may be made orally, without written authorizations for use or disclosure for these two purposes.

To disclose PHI for these purposes, covered entities must inform individuals in advance and must provide a meaningful opportunity for the individual to prevent or restrict the disclosure.

In certain exceptional circumstances, such as in an emergency, when this informal discussion cannot practicably occur, covered entities can make decisions about disclosure or use, in accordance with the requirements of Section §164.510 based on their professional judgment of what is in the individual’s best interest or consistent with prior preference.

## Policies and Procedures

The preamble to the HIPAA Privacy Rule discusses in detail the requirements in §164.510 for complying with this standard. The policies and procedures regarding uses and disclosures of protected health information allows for a person to agree or object in the two circumstances discussed below.

Section §164.510 (a) – Use and Disclosure for Facility Directories: Covered health care providers, specifically health care facilities, are allowed to include limited information in their directory only if:

- They inform incoming individuals of their policies regarding the directory;
- They give individuals a meaningful opportunity to opt out of the directory listing or to restrict some or all of the uses and disclosures that can be included in the directory; and
- The individual does not object to being included in the directory.

The facility's notice and the individual's opt-out or restriction may be oral.

A covered health care provider, subject to the individual's right to object or known prior expressed preferences, is permitted to disclose the following information to persons who inquire about the individual by name:

- The individual's general condition in terms that do not communicate specific medical information about the individual (e.g., fair, critical, stable, etc.); and
- Location in the facility.

A covered entity is permitted, subject to the individual's right to object to or restrict disclosure, to disclose directory information to a member of clergy, even if the clergy does not inquire by the individual's name:

- The individual's name;
- The individual's general condition in terms that do not communicate specific medical information about the individual;
- The individual's location in the facility; and
- The individual's religious affiliation.

A health care provider does not have to inquire about an individual's religious affiliation and the individual is not required to disclose their religious affiliation to be included in the facility directory.

There are certain circumstances under which health care facilities can use or disclose specified health information for the facility directory without the individual's agreement. Disclosures are allowed when the individual is incapacitated or in emergency treatment circumstances, when asking permission would delay treatment such that the individual's health would be jeopardized. The individual must be given the opportunity to object to uses or disclosures in the directory when it is practicable to do so.

The covered entity (CE) must determine whether to include an incapacitated individual's information in the facility's directory based on professional judgment as to the individual's best interests or known preferences. The CE can decide to disclose some information (name) but not other information (location) to protect the individual's interests.

When the individual is not able to make a decision regarding inclusion or exclusion in the facility directory factors to take into consideration whether to include an individual's information in the facility directory are:

- Whether disclosing that the individual is in the facility could reasonably cause harm or danger to the individual;
- Whether disclosing an individual's location within the facility could give information about the individual's condition; Whether it is necessary or appropriate to give information to family or friends;
- Whether the individual had, prior to becoming incapacitated, expressed a preference regarding inclusion or exclusion in the facility directory.

When the individual's condition stabilizes such that he or she is capable of decision-making, a covered health care provider must, when it becomes practicable, inform the individual about its policies regarding the

facility's directory and provide the opportunity to object to the use or disclosure of protected health information about themselves for the directory.

### **Section §164.510(b)(1-3) – Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes**

Covered health care entities may disclose to a person involved in the current health care of the individual (such as family member, other relative, close personal friend, or any other person identified by the individual) protected health information directly related to the person's involvement in the current health care of the individual or payment related to the individual's health care.

It is not a requirement to verify the identity of relative or other individuals involved in the individual's care. The individual's act of involving the other persons in his or her care suffices as verification of their identity.

Protected health information may be disclosed by a covered entity to notify or assist in notification of family members, personal representatives, or other persons responsible for an individual's care with respect to an individual's location, condition, or death.

Only the minimum information necessary should be disclosed when a covered entity could not practicably obtain oral agreement to disclose protected health information to next-of-kin, relatives, or those with a close personal relationship to the individual and the covered entity should make such disclosures consistent with good health professional practice and ethics.

It cannot be assumed that an individual's agreement at one point in time to disclose protected health information to a relative or to another person assisting in the individual's care implies agreement to disclose protected health information indefinitely in the future. However, if the individual is routinely accompanied by the same person (spouse, child, etc.) when treatment is discussed a provider can infer that that person is playing a long-term role in the individual's care and that disclosure of PHI consistent with the person's role in the individual's care is appropriate.

### **Disclosure When the Individual is Present**

When the individual is present and has the capacity to make his or her own decisions, protected health information may be disclosed only if:

- The individual's agreement is obtained to disclose to the third parties involved in their care;
- The individual is provided with an opportunity to object to such disclosure and the individual does not express an objection; or
- It is reasonably inferred from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure, such as when a individual brings a spouse into the doctor's office when treatment is discussed or when a colleague or friend has brought the individual to the emergency room for treatment.

### **Disclosure When the Individual is Not Present**

When the individual is not present or is incapacitate and not able to participate in decision making, it must be determined whether the disclosure is in the individual's best interests and if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

- Covered entities may disclose functional information to individuals assisting in an individual's care (for example, disclosing mobility limitations to a friend driving the individual home from the hospital).
- Professional judgment and experience with common practice may be used to make reasonable inferences of the individual's best interest in allowing a person to act on an individual's behalf to pick up filled

prescriptions, medical supplies, X-rays and similar forms of protected health information. For example, if a person comes to a pharmacy and asks to pick up a specific prescription for an individual, it effectively verifies that they are involved in the individual's care and the pharmacist can give the medication to that person.

- Information should not be disclosed to a suspected abuser, if there is reason to believe that such a disclosure could put the individual at risk of serious harm.

Disclosure of PHI to others involved in care should be limited to that pertinent to the individual's current health and treatment and should not include past PHI that is not relevant to the individual's current health.

#### **Disclosure for Disaster Relief Activities§164.510(b)(4)**

Protected health information may be disclosed to federal, state, or local government agencies engaged in disaster relief activities, as well as to private disaster relief or disaster assistance organization (such as the Red Cross) authorized by law or by their charters to assist in disaster relief efforts.

Disclosures to disaster relief agencies are subject to the same requirements to inform the individual and give them an opportunity to agree or object to the disclosure of their PHI with exceptions that are allowed in emergency circumstances. Information disclosed must be limited to the minimum necessary to needed for disaster relief purposes.

Note: There is no need for a Business Associate Agreement with disaster relief agencies, as they are not using PHI to perform a service on behalf of the CE disclosing the PHI.

### **Policies and Processes to Implement the Standard**

#### **Facility Directory**

- Define the facility directory; is it only inpatients, does it include individuals registered for ambulatory surgery, infusion centers, and emergency department.
- At what step in the registration/admission process and by what staff role(s) will the individual be provided information about the facility directory and asked about their preference.
- How will the preference be documented and communicated so the pertinent stakeholders are aware of preferences.
- What process might be available to document the individual's preferences so it would be known if the individual is ever incapacitated and not able to make their wished known regarding the directory.
- How will processes that currently rely on facility directory information be handled in the future, for example flower delivery?

#### **Involved in Care**

- Determine what approach the CE will take in obtaining the individual's agreement to disclose PHI to others involved in care. What role's responsibility is it and at what point(s) in the care process will this occur?
- Guidelines and training to assist staff in making decisions regarding disclosures to those involved in care when the individual is not present/incapacitated; to whom, under what circumstances, limited to relevant PHI.

#### **Disaster Relief**

Consider incorporating statements about disclosing PHI to disaster relief agencies in the organization's Disaster Planning or Mass Casualty policies;

- When and by what role will an individual be asked about disclosures to disaster relief agencies;
- Who may disclose the information to a disaster relief agency;
- Verifying the role of the relief agency (authorized by law or charter to receive information);
- Minimum PHI to be disclosed.

# Use and Disclosure - Research Activities

Revision Date: 09/30/2002

## Citations

The following sections of the Privacy regulation and its preamble set the standards for the use and disclosure of information for research activities and the policies and procedures required to implement these standards:

- §164.508 – Uses and disclosures for which an authorization is required
- §164.512(i) – Uses and disclosures for which an authorization, or opportunity to agree or object is not required: uses and disclosures for research purposes
- §164.514(d) – Minimum necessary uses of protected health information
- §164.514(e) – Limited Data Set
- §164.524 – Access of individuals to protected health information
- §164.528 – Accounting of disclosures of protected health information
- §164.532 – Transition provisions
- December 2000 Preamble, Federal Register pg. 82535 - 82538 and 82689 - 82703 – Discussion of uses and disclosures for research purposes
- Modifications to the HIPAA Privacy Rule, Federal Register pg. 53224 - 53226 – Research Authorizations

## General Requirements

Protected health information (PHI) used or created for research is subject to the HIPAA Privacy Rule. The Rule specifies conditions under which a covered entity may use and disclose PHI for research purposes.

The following research is *not* subject to HIPAA:

- Research using health information that meets the Privacy Rule's de-identification standards

Research that does not access the covered entity's medical record and does not create PHI in the course of the research

§164.508 covers the standards for:

- Authorizations for uses and disclosures
- Required elements of authorizations
- Revocation of authorizations

Research authorizations, like all authorizations, must specifically describe what information may be used and disclosed and the circumstances under which the use and disclosure will be made. A research authorization may be combined with other written permission for the same research study..

§164.512 covers the uses and disclosures for which an authorization, or opportunity to agree or object are not required. Section 512(i) outlines three circumstances under which covered entities may disclose PHI for research purposes without obtaining individual authorization.

§164.514(d) presents the principle of minimum necessary uses and disclosures. With certain exceptions, covered entities must limit uses and disclosures of information to that which is reasonably necessary to accomplish the purpose for which the request was made.

§164.514(e) allows the development of a limited data set for research purposes. The Modified HIPAA Rule specifies the direct identifiers that must be removed before protected health information will be considered a limited data set. Covered entities may disclose limited data sets to researchers only upon receipt of a data use agreement.

§164.524 specifies the circumstances under which an individual's right to access to health information may be suspended or denied. It also requires that there be procedures for individuals to request access and to appeal denial of access.

§164.528 establishes the individual's right to request an accounting of disclosures made by a covered entity. Certain research disclosures must be included in the accounting.

§164.532 allows the use and disclosure of PHI in an ongoing research project after April 14, 2003, provided that the individual has already signed a legal permission or consent form, or an IRB has waived the consent requirement

## **Policies and Procedures**

### **Uses and Disclosures for Which An Authorization Is Required (§164.508)**

A covered entity may condition research-related treatment on the provision of an authorization.

The authorization for uses and disclosures of protected health information must contain:

- A specific description of the purpose of the authorization and the information to be used or disclosed
- The names or classes of individuals authorized to make the use or disclosure
- The names or classes of individuals authorized to receive the use or disclosure
- An expiration date for the authorization The statement "end of research study", "none" or similar language is sufficient for research purposes.
- A statement that the individual has a right to revoke the authorization
- A reference to the covered entity's right to condition service on the authorization, or the consequences of refusal to sign.

A statement that the information used or disclosed pursuant to the authorization may be subject to re-disclosure and no longer protected by the Privacy Rule.

The authorization must be written in plain language.

A research authorization may be included in the consent form to participate in the same research study.

### **Uses and Disclosures For Which Authorization, or Opportunity To Agree or Object Is Not Required (§164.512)**

Section 164.512 outlines three conditions under which a covered entity may use or disclose protected health information for research without written authorization from the individual:

**1. Board approval of a waiver of authorization**, provided that:

- There is an Institutional Review Board (IRB) established in accordance with appropriate federal regulations or a Privacy Board comprised of appropriate members as specified in the rule;

- The IRB or Privacy Board approves a waiver of authorization; and
- The covered entity obtains documentation that the board has approved an alteration to the individual authorization or waiver of all or part of the authorization.

The approval of a waiver must include the following:

- 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
- Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver of authorization satisfies the three criteria specified in §164.512(i)(2)(ii)
- 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
- A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures
- Signature of the chair or other member designated by the chair, of the IRB or the Privacy Board

**2. Reviews preparatory to research.** The researcher must attest that:

- The information is being sought solely to prepare a research protocol or for similar purposes preparatory to research.
- No protected health information is to be removed from the covered entity by the researcher.

The information being sought is necessary for research purposes.

**3. Research on decedents information.** The researcher must attest that:

- The information being sought is solely for research on decedents
- The information being sought is necessary for research purposes
- The covered entity has a right to require documentation of the death of the individuals.

**Limited Data Set (§164.514)**

New provisions in the Modification to the HIPAA Privacy Rule establish a fourth mechanism by which a covered entity may use and disclose PHI for research purposes without written authorization from the individual. Covered entities, or their business associates, may create a limited data set that excludes direct identifiers, but still contains potentially identifying information. Use or disclosure of a limited data set is conditioned upon the receipt of a data use agreement. Under these circumstances, waiver of authorization by an IRB or Privacy Board is not required.

A limited data set must adhere to the minimum necessary provisions of the Rule.

Unlike disclosures made under 164.512(i), disclosures made in a limited data set do not have to be included in the covered entity's accounting of disclosures to an individual.

**Minimum necessary uses of protected health information (§164.514)**

The minimum necessary standard applies to uses and disclosures for research purposes. When making disclosures of protected health information related to research, the covered entity may rely on documentation from researchers that the information requested is the minimum necessary to accomplish the research purpose. This requirement applies to research information disclosed without individual authorization. Uses and disclosures pursuant to a valid research authorization are exempt from the minimum necessary standard.

**Access of Individuals to Protected Health Information (§164.524)**

An individual's access to protected health information 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, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

### **Accounting of Disclosures of Protected Health Information (§164.528)**

Individuals have a right to receive an accounting of disclosures of protected health information made by a covered entity. Certain exceptions apply: the covered entity is not required to account for disclosures made pursuant to an authorization or disclosures in a limited data set. Disclosures made by waiver of authorization, preparatory to research, or concerning decedents must be included in the accounting.

For research disclosures that require accounting, the Modifications to the HIPAA Privacy Rule offer the option of a simplified accounting method. If the research project involves more than 50 records, the covered entity may provide individuals with a list of research protocols for which the individual's protected health information might have been disclosed. The list must include the name of the study, a description of the purpose of the study, the type of information sought, and the timeframe of the disclosure. When requested, the covered entity must assist the individual in contacting the researcher to whom it is likely that the individual's protected health information was actually disclosed.

### **Transition Provisions (§164.532)**

The Privacy Rule allows the continued use and disclosure of protected health information in ongoing research projects provided that the individual has already signed a legal permission or consent form, or an IRB has waived the consent requirement, prior to the compliance date. The legal permission must identify the specific research project in question.

In making such uses and disclosures, the covered entity must comply with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

### **Miscellaneous Considerations and Issues**

Covered entities that use and disclose protected health information for research purposes must institute new processes for the following activities:

- stripping identifiers to provide de-identified data for research
- extracting a limited data set
- reviewing the adequacy of data use agreements
- reviewing the validity of research authorizations
- accounting for research disclosures
- reinstating individual access to research-related information upon completion of the research
- educating IRB and faculty about HIPAA research provisions
- educating faculty and study coordinators about informing research subjects of privacy considerations specific to research

# Use and Disclosure - Underwriting and related purposes

Revision Date: 10/10/2002

## Citations

The following sections of the Privacy Rule and its preamble address the issue of use and disclosure of protected health information for underwriting and related purposes:

- Preamble, pg. 82513-16 and 82743 – Discussion of uses and disclosures requiring authorization
- Preamble, pg. 82546 – Discussion of uses of PHI for underwriting
- §164.504(f) – Uses and disclosures: organizational requirements (*standard requirements for group health plans*)
- §164.508(a) – Uses and disclosures for which authorization is required: Standard - general rules
- §164.508(b)(4)(ii)(A) and (B) – Prohibition on conditioning of authorizations (*exceptions*)
- §164.514(g) – Other requirements relating to uses and disclosures of protected health information – Standard – Uses and disclosures for underwriting and related purposes
- §164.528 – Accounting Of Disclosures Of Protected Health Information

## General Requirements

The definition of health care operations was expanded in the final rule to include underwriting and risk determination. The regulations require a health plan to obtain an authorization for use of PHI in underwriting and risk determination of a new applicant. A health plan may condition enrollment upon receipt of the authorization. As an exception to this regulation enrollment may not be conditioned on psychotherapy notes.

§164.508(a) – Uses and disclosures for which authorization is required: Standard - general rules: (*Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization*). This section sets the requirement for an authorization for use of PHI by a health plan in its underwriting or risk determination. The requirement to obtain authorization is explicitly stated in the preamble discussion on page 82514 under the heading “pre-enrollment underwriting.” This discussion notes that if the individual applies for renewal of existing coverage, the health plan would not need to obtain an authorization in order to review its existing claim records for that individual. This activity comes under the definition of health care operations and is permissible. In addition, a group health plan may disclose summary health information for purposes of obtaining premium bids without an authorization under §164.504(f).

§164.508(b)(4)(A) and (B) – Prohibition on conditioning of authorizations: This section sets forth the prohibitions (and exceptions) on conditioning of authorizations. Paragraph (A) of this section specifically allow health plans to condition enrollment on obtaining an individual’s authorization to use PHI for underwriting or risk determination. Paragraph (B) excludes psychotherapy notes from this exception, so a health plan may not condition enrollment on an authorization for psychotherapy notes.

§164.514(g) – Other requirements relating to uses and disclosures of protected health information – Standard – Uses and disclosures for underwriting and related purposes. This section clearly and unambiguously states: “*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.”*

§164.504(f) – Uses and disclosures: organizational requirements: This section lists conditions under which summary information may be shared with a plan sponsor. Paragraph (1)(ii) of this section authorizes an insurer or HMO to disclose summary information to a plan sponsor for purposes of (A) obtaining premium bids, and for (B) modifying, amending or terminating a group health plan.

§164.528 – Accounting Of Disclosures Of Protected Health Information: This section sets forth the requirements for reporting any uses or disclosures of PHI. For the purposes of underwriting, this accounting requirement exists only when an authorization is required. The disclosure of PHI to a covered entity (insurer) for underwriting is further discussed in the comments section on page 82743 clarifying the use of summary accounting for a series of disclosures.

## **Policies and Procedures**

A covered entity will need policies and procedures covering the use of PHI for underwriting and risk determination for health plans. These policies and procedures should take into consideration the following points from the preamble:

- Requires an individual to sign an authorization for the covered entity to use PHI for underwriting or risk determination prior to enrollment (page 82514) in a health plan. Enrollment may be made contingent on this authorization except that enrollment may not be made contingent on an authorization for psychotherapy notes.
- Section 164.504 (f) requires that any information collected under this authorization may not be used for any other purpose if the individual is not enrolled.
- Section 164.528 sets forth the requirement for providing an individual an accounting of disclosures. See comment on page 82743 regarding use of summary accounting for a series of disclosures.

# Use and Disclosure - Verification of Identity and Authority of Entities Requesting PHI

Revision Date: 10/08/2002

## Citations

One section of the Privacy regulation and its preamble address the verification of the identity and authority of those requesting PHI. Three other sections make references to verification for uses:

- §164.514(h) – Other Procedural Requirements Relating to Uses and Disclosures of Protected Health Information – Standard: Verification requirements
- §164.512(a) – Uses and disclosures for which consent, an authorization or object is not required – Standard: Uses and disclosures required by law
- §164.512(f) – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required – Standard: Disclosures for law enforcement purposes.
- §164.502(f) – Uses and disclosures of protected health information: general rules – Standard: Deceased individuals.
- §164.510(b) – Uses and disclosures requiring an opportunity for the individual to agree or to object: Standard: Uses and disclosures for involvement in the individual’s care and notification purposes
- Preamble, pg. 82546-7 and pg. 82718-20 – Discussion of verification of identity and authority of persons requesting PHI

## General Requirements

In §164.514(h) “a covered entity must verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to the covered entity.”

In §164.514(h) a covered entity must “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.”

An exception to this Standard is covered under §164.510 which specifies uses and disclosures requiring an opportunity for the individual to agree or to object to disclosures for facility directories and for uses and disclosures for involvement in the individual’s care and notification purposes.

## Policies and Procedures

The preamble of the Privacy Rule discusses in detail the requirements for verification of identity and authority of persons requesting protected health information.

The covered entity must establish and use written policies and procedures (which may be standard protocols) that are reasonably designed to verify the identity and authority of the requestor where the covered entity does not know the person requesting the protected health information.

The knowledge of the person may take the form of:

- A known place of business;
- A known address;
- A known phone or fax number; or
- A known human being.

Where documentation, statements or representations, whether oral or written, from the person requesting the protected health information is a condition of disclosure, the covered entity must obtain these documentation statements or representations prior to disclosing the requested information.

Additional verification is only required where this regulation (or other law) requires additional proof of authority and identity.

### **Policies and Procedure for Verifying Public Officials**

Where the person requesting the protected health information is a public official, covered entities 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:

- If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- If the request is in writing, the request is on the appropriate government letterhead; or
- 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.

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 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; or
- 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.

§164.512(a) addresses the uses and disclosures required by law that specifies when a covered entity must disclose protected health information to public officials. §164.501 defines law enforcement official and what is "required by law."

Disclosure to the Secretary is required for purposes of enforcing the Privacy regulation. When protected health information is requested by the Secretary for compliance purposes, the covered entity must verify the identity of the requestor and their authority to access protected health information as would be required for any other law enforcement or oversight agency request for disclosure.

### **Policies and Procedures When Verification Is Not Required**

If there is an imminent threat to safety, it is lawful to disclose private health information to prevent or lessen a serious and imminent threat to the health or safety of a person or the public if disclosure is made to a person reasonably able to prevent or lessen the threat. If these conditions are met, no further verification is needed.

In such emergencies, the covered entity is not required to demand written proof that the person requesting the protected health information is legally authorized. Reasonable reliance on verbal representations is appropriate.

### **Policies and Procedures for Verifying Persons Assisting in an Individual's Care**

A covered entity is required to verify the identity and authority of persons assisting in an individual's care before disclosing protected health information. Procedures for disclosures to persons assisting in an individual's care are discussed in §164.510(b).

### **Policies and Procedures for Verifying an Individual When Requesting Their PHI**

A covered entity is required to give an individuals access to his/her protected health information (under most circumstances). A covered entity is required to take reasonable steps to verify the identity of the individual making the request. No particular identification requirements are mandated (e.g., drivers license, photo ID); it is left up to the discretion of the covered entity.

### **Policies and Procedures for Verification of a Personal Representative**

A covered entity must establish and document procedures for verification of identity and authority of personal representatives, if not known to the entity. A healthcare provider can:

- Require a power of attorney; or
- Ask questions to determine that an adult acting for a young child has the requisite relationship to the child.

### **Policies and Procedures for Verification for Use for Research Purposes**

In §164.502(f) protected health information of a deceased individual sought for research purposes requires that covered entities obtain an oral or written representation that the protected health information will be used or disclosed solely for research. A definition of "research" is provided in §164.501. §164.512 (i)(1)(iii) requires the covered entity to obtain from the researcher documentation of the death of the individual.

### **Policies and Procedures for Verification of Next of Kin**

The covered entity is required to verify the identity and authority of persons requesting protected health information, including in next of kin situations, where the identity or authority of such person is not known to the covered entity. Procedures for disclosures to next of kin and other family members are discussed in §164.510(b), which allows the covered entity to exercise professional judgment as to whether the disclosure is in the individual's best interest when the individual is not available to agree to the disclosure or is incapacitated.

### **Policies and Procedures for Verification in Underwriting and Related Purposes**

Covered health care providers are required by the final rule to adhere to current best practices for verification when the covered provider does not know the requester. The provider must make a reasonable effort to determine that the protected health information is being sent to the entity authorized to receive it. Current practices of sending the information to a recognizable organizational address or, if axing or phoning information, by calling the requester back through the main organization switchboard rather than through a direct phone number, are sufficient to meet the relevant requirement of the final rule.

**Policies And Procedures Regarding Personal Representatives.**

See section: Privacy Policies and Procedures: Personal

# Use & Disclosure - Victims of Abuse, Neglect, Domestic Violence, and Crime

Revision Date: 09/06/ 2002

## Citations

The following sections of the Privacy rule and its preamble address the issues of disclosures involving crime victims, abuse and domestic violence:

- §164.512 (b)(1)(ii) – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required – Standard: uses and disclosures for public health activities – Permitted disclosures
- §164.512 (c) – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required – Standard: Disclosures about victims of abuse, neglect or domestic violence
- §164.512 (f)(3) – Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required – Standard: Disclosures for law enforcement purposes – Permitted disclosure: Victims of a crime
- §164.528 (b) – Accounting of disclosures of protected health information – Implementation specifications: Content of the accounting
- §164.528 (d) – Accounting of disclosures of protected health information – Implementation specifications: Documentation
- Preamble, pg 82524 – 82534 - Discussion of §164.512 (a)-(f)
- Comments pg. 82668 – 82687 – Discussion of comments regarding §164.512 (b) – (f)
- Comments, pg. 82741 – Comments regarding §164.528

## General Requirements

### Child Abuse

Covered entities are permitted to disclose protected health information to report child abuse or neglect to a public health authority or other appropriate government authority.<sup>13</sup> It is not necessary to obtain consent or authorization or allow the individual an opportunity to agree or object to this disclosure. The covered entity is not required to inform the victim of the disclosure.

### Victims of Abuse, Neglect, Domestic Violence

§164.512(c) of the Privacy regulation establishes the general standard regarding disclosures about victims of abuse, neglect or domestic violence. In addition to reporting child abuse, the rule states that a covered entity may disclose to a governmental authority protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence. There are three circumstances in which the covered entity may disclose protected health information about these victims.

---

<sup>13</sup> §164.512(b)(1)(ii) Federal Register, Vol. 65, No. 250, Thursday, December 28, 2000, Rules and Regulations.

- 1) Law requires disclosure related to abuse and the disclosure must comply with and is limited to the relevant requirements of such law.
- 2) The individual has agreed to such disclosure
- 3) The disclosure is expressly authorized by statute or regulation and either:
  - a) The covered entity believes that disclosure is necessary to prevent serious harm to the individual or to other potential victims; or
  - b) If the individual is unable to agree due to incapacity, the law enforcement or public official authorized to receive the report represents that the information sought is not intended to be used against the individual, and that an immediate enforcement activity would be materially and adversely affected by waiting.

In these situations, the covered entity is required to promptly inform the victim that it has disclosed protected health information to report abuse, neglect, or domestic violence. However, the covered entity can elect not to inform the victim if it believes that receiving this information places the victim in jeopardy. The covered entity is not required to inform a personal representative if it believes that person is responsible for the abuse, neglect or other injury that has already occurred and that informing that person would not be in the individual's best interests.

### **Victims of a Crime**

In addition to disclosures related to child abuse and victims of abuse, neglect or domestic violence, §164.512(f)(3) of the Privacy regulation permits disclosures for victims of a crime. In some cases state or other law may mandate disclosure. Except for disclosures required by law, covered entities are required to obtain individual agreement as a condition of disclosing the protected health information about victims to law enforcement.

The individual agreement requirement is waived if the covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

- The law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred, and this information is not intended to be used against the victim;
- The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be harmed by waiting until the individual is able to agree; and
- The covered entity believes the disclosure is in the best interests of the individual.

## **Policies and Procedures**

### **Victims of Abuse, Neglect, and Domestic Violence**

The final HIPAA Privacy Rule allows covered entities to disclose protected health information about an individual whom it reasonably believes to be a victim of abuse, neglect, or domestic violence. The provisions apply to such situations as abuse of nursing home residents, abuse of residents of facilities for the mentally retarded; and domestic violence. HIPAA addresses child abuse specifically in connection with a State's public health activities. State laws continue to apply with respect to child abuse, and the final HIPAA Privacy Rule does not in any way interfere with a covered entity's ability to comply with these laws.

The rule allows such disclosure to any governmental authority authorized by law to receive reports of such abuse, neglect, or domestic violence. The three circumstances in which this disclosure is allowed are given in

the general requirements section above. It is emphasized in both the preamble and comments discussion of §164.512(c) that it is important for the covered entity to notify the individual when protected health information is disclosed to authorized government authorities. The covered entity is allowed to provide the information orally. Written notification is not required and sometimes might be harmful due to the sensitivity of abuse situations and the potential for the abuser to cause further harm to the individual, if for example, a covered entity sends written notification to the home of the individual and the abuser.

The rule requires that the disclosures be documented and the documentation retained for six years. The specific items that must be documented are listed below.

To implement the appropriate disclosures involving victim's of abuse, neglect, and domestic violence, the covered entity must:

- 1) Determine and follow the requirements of state and local law regarding victims of abuse, neglect, and domestic violence.
- 2) For child abuse cases follow state and local law.
- 3) Ascertain if there is evidence that the individual is a victim of abuse, neglect, or domestic violence.
- 4) Make disclosure to appropriate governmental authorities as required by law.
- 5) Seek agreement from the individual (victim) if possible before making such disclosures.
- 6) If the agreement has not been obtained, use professional judgment to determine if notification of the individual could possible cause harm or not be in his best interest.
- 7) Notify the individual, if possible and appropriate, of any such disclosures.
- 8) If written documents are used to notify the individual, take care that these documents will not instigate harmful consequences.
- 9) Make appropriate documentation and retain it for six years. Proper documentation is to include:
  - a) The date of the disclosure
  - b) The name and address, if known, of the entity or person who received the protected health information
  - c) A brief description of the protected health information disclosed
  - d) A brief statement of the purpose of the disclosure
  - e) A copy of an authorization, if obtained
  - f) A copy of a written request for disclosure
  - g) Documentation of oral communication with the individual is desirable.

### **Victims of Crime**

The final HIPAA Privacy Rule requires covered entities to obtain individual agreement as a condition of disclosing the protected health information about victims to law enforcement. The exception to this rule is if State or other law mandates the disclosure of protected health information. The required agreement may be obtained orally and does not have to meet the requirements established for HIPAA Authorizations. If the victim is unable to agree due to incapacity or other emergency circumstance, the rule waives the requirement for the individual agreement. However, in order to disclose protected health information to law enforcement in this circumstance, the law enforcement official must represent that the information sought is needed to determine whether a violation of law by a person other than the victim has occurred, and that the information is not intended to be used against the victim. The law enforcement official must also represent that waiting

until the individual is able to agree to the disclosure would materially and adversely affect immediate law enforcement activity. The covered entity also in its best judgment must determine that the disclosure is in the individual's best interest. It is important to note that the provision does not allow covered entities to initiate disclosures of protected health information to law enforcement; the disclosure must be in response to a request from law enforcement, and the minimum necessary standard applies to any such disclosures. If the individual is a suspect, covered entities may disclose the protected health information pursuant to §164.512(f)(3) regarding suspects.

The rule requires that the disclosures be documented and retained for six years. The specific items that must be documented are listed below.

To implement the appropriate disclosures involving victims of crime, the covered entity must:

- 1) Determine and follow the requirements of state and local law regarding victims of crime.
- 2) If state or local law does not require mandatory disclosure, obtain the individual's agreement before making the disclosure.
- 3) This agreement may be obtained orally or in written fashion.
- 4) If the victim is unable to agree due to incapacity or emergency circumstance, the covered entity must use its best judgment as to what is in the victim's best interest. The law enforcement official must represent that the information is immediately necessary, and that the information will not be used against the individual.
- 5) Make appropriate documentation and retain it for six years. Proper documentation is to include:
  - a) The date of the disclosure
  - b) The name and address, if known, of the entity or person who received the protected health information
  - c) A brief description of the protected health information disclosed
  - d) A brief statement of the purpose of the disclosure
  - e) A copy of an authorization, if obtained
  - f) A copy of a written request for disclosure
  - g) Documentation of oral communication with the individual is desirable.

# Appendix A: Privacy and Security Terminology

Revision Date: 09/06/2002

- **Audit trail** – data collected and potentially used to facilitate a security audit, to include the who (login ID), what (read-only, modify, delete, add, etc.), and when (date/timestamp).
- **Audit controls** – the mechanisms employed to record and examine system activity.
- **Authorization** – permission granted by the patient or the patient’s personal representative to use or disclose protected health information for purposes other than treatment, payment, health care operations or uses and disclosures permitted or required by the Privacy Rule.
- **Access**- the ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.
- **Access Authorization** – Information–use policies/procedures that establish the rules for granting and/or restricting access to a user, terminal, transaction, program, or process.
- **Access Control** – A method of restricting access to resources, allowing only privileged entities access. (PGP, Inc.) Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation.
- **Access Controls** – The protection of sensitive communications transmissions over open or private networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient.
- **Access Establishment** – The security policies, and the rules established therein, that determine an entity’s initial right of access to a terminal, transaction, program, or process. Part of information access control on the matrix.
- **Access Level** – A level associated with an individual who may be accessing information (for example, a clearance level) or with the information that may be accessed (for example, a classification level).
- **Access Modification** – The security policies, and the rules established therein, that determine types of, and reasons for, modification to an entity’s established right of access to a terminal, transaction, program, or process.
- **Accountability** – The property that ensures that the actions of an entity can be traced uniquely to that entity. (ASTM E1762 - 95). (#)
- **Business associate** – A person who on behalf of a covered entity (or of an organized health care arrangement in which the covered entity participates) performs, or assists in the performance of:
  - A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
  - Any other function or activity regulated by this subchapter; or

- A person who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity (or to or for an organized health care arrangement in which the covered entity participates) where the provision of the service involves the disclosure of individually identifiable health information from such covered entity (or arrangement), or from another business associate of such covered entity (or arrangement), to the person.
- **Biometric identification** – An identification system that identifies a human from a measurement of a physical feature or repeatable action of the individual, such as, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature. (§142.308(c)(1)(v) HHS HIPAA Security NRPM)
- **Classification based access control** – Protection of data from unauthorized access by the designation of multiple levels of access authorization clearances to be required for access, dependent upon the sensitivity of the information.
- **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.
- **Consent** – Permission granted by the patient or the patient’s guardian to use or disclose protected health information for purposes of treatment, payment or health care operations.
- **Covered entities** –
  - A health plan (as defined in 45 C.F.R. §160.103).
  - A health care clearinghouse.
  - A health care provider who transmits any health information in electronic form in connection with a transaction covered by this HIPAA’s Administrative Simplification provisions.
- **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.
- **Designated record set** – A group of records maintained by or for a covered entity that includes the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or used, in whole or in part, by or for the covered entity to make decisions about individuals. For purposes of this definition, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
- **De-identified information** – Health information that meets the standard and implementation specifications under 45 C.F.R. §164.514 (a) and (b).
- **Digital signature** – An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. (FDA Electronic Record; Electronic Signatures; Final Rule)
- **Disaster recovery** – The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. (CPRI, 1996c, as cited in HISB,

DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)

- **Disclosure** – The release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.
- **Discretionary Access Control (DAC)** – is used to control access by restricting a subject's access to an object. It is generally used to limit a user's access to a file. In this type of access control it is the owner of the file who controls other users' accesses to the file.
- **Double keying** – The act of key entering data twice to ensure the accuracy of the data entered.
- **Electronic data interchange (EDI)** – Intercompany, computer-to-computer transmission of business information in a standard format. For EDI purists, "computer-to-computer" means direct transmission from the originating application program to the receiving, or processing, application program, and an EDI transmission consists only of business data, not any accompanying verbiage or free-form messages. Purists might also contend that a standard format is one that is approved by a national or international standards organization, as opposed to formats developed by industry groups or companies. (EDI Security, Control, and Audit)
- **Encryption** – Transforming confidential plaintext into cipher text to protect it (also called encipherment). An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over unsecured lines. (EDI Security, Control, and Audit)
- **Emergency mode operation** - Access controls in place that enable an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
- **Entity authentication** – 1. Processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network (§142.308(d) HHS HIPAA Security NRPM). 2. A communications/network mechanism to irrefutably identify authorized users, programs, and processes, and to deny access to unauthorized users, programs and processes. (§142.308(d)(2)(iii) HHS HIPAA Security NRPM)
- **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.
- **Facility security plan** – A plan to safeguard the premises and building(s) (exterior and interior) from unauthorized physical access, and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.
- **Fundraising** – An activity of a covered entity intended to raise funds to benefit the covered entity or an institutionally related foundation that has as its mission to benefit the covered entity.

**Group Health Plan** – An employee welfare benefit plan, including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise

**Guideline** – a policy or rule intended to give practical guidance.

- **Health care operations** – Any of the following activities (see 45 C.F.R. §164.501) of the covered entity to the extent that the activities are related to covered functions, and:
  - Conducting quality assessment and improvement activities;
  - Reviewing the competence or qualifications of health care professionals
  - Underwriting, premium rating
  - Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
  - Business planning
  - Business management and general administrative activities of the entity
- **HHS or Secretary** – the Department of Health and Human Services or the Secretary of Health and Human Services.
- **Health information** – Any information, oral or recorded in any medium, that:
  - Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
  - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
- **Hybrid entity** – Means a single legal entity that is a covered entity and whose covered functions are not its primary functions.
- **Implementation Specification** – Specific requirements or instructions for implementing a standard.
- **Individual** – The person who is the subject of protected health information.

**Individually identifiable health information** -- Means information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

- **Information access control** – Formal, documented policies and procedures for granting different levels of access to health care information.
- **IRB-** Institutional Review Board, established to review research activities in accordance with federal regulations.
- **Internal audit** – The in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an organization.

**Limited data set.** Means protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual identified in 45 C.F.R. 164.514(e).

- **Mandatory Access Control (MAC)** – A means of restricting access to objects that is based on fixed security attributes assigned to users and to files and other objects. The controls are mandatory in the sense that users or their programs cannot modify them.

**Marketing** means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made: (i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or (ii) For treatment of the individual; or (iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. Marketing also means an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

- **Message authentication code** – Data associated with an authenticated message that allows a receiver to verify the integrity of the message. (Glossary of INFOSEC and INFOSEC Related Terms - Idaho State University)
- **Minimum necessary** – When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity generally must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
- **Need-to-know** – A security principle stating that a user should have access only to the data he or she needs to perform a particular function
- **Password** – A confidential numeric and/or character string used in conjunction with a User ID to verify the identity of the individual attempting to gain access to a computer system.
- **Payment** – The activities undertaken by either a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a covered health care provider or health plan to obtain or provide reimbursement for the provision of health care.
- **Personal identification number (PIN)** – A number or code assigned to an individual and used to provide verification of identity.
- **Plan** – a detailed scheme or method for the accomplishment of an object.
- **Plan Administration Functions** – 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.
- **Plan Sponsor** – The employer in the case of an employee benefit plan established or maintained by a single employer, the employee organization in the case of a plan established or maintained by an employee organization, or in the case of a plan established or maintained by two or more employers or jointly by one or more employers and one or more employee organizations, the association, committee, joint board of trustees, or other similar group of representatives of the parties who establish or maintain the plans.

- **Policy** – A general principle or plan that guides the actions taken by an individual or group.
- **Procedure** – A way of performing or accomplishing something; a series of steps; course of action.
- **Process** – A series of steps, actions or operations used to bring about a desired result.
- **Protected health information** – Individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form that is (1) Created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.
- **Research** – Means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
- **Role-based access control** – Role-based access control (RAC) 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.
- **Standard** – A rule, condition, or requirement describing the following information for products, systems, services or practices: classification of components, specification of materials, performance, or operations; or delineation of procedures; or with respect to the privacy of individually identifiable health information.
- **Summary Health Information** – Information, that may be individually identifiable health information, and:
  - 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
  - From which the identifiers of the individual or of relatives, employers, or household members of the individual specified in 45 C.F.R. §154.504(a), are removed
- **Technical security mechanisms** – 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. (§142.308(d)(2) HHS HIPAA Security NRPM)
- **Time-of-day access control** – Access to data is restricted to certain periods, e.g., Monday through Friday, 8:00 a.m. to 6:00 p.m.
- **Token** – A physical item containing an electronic device used to provide identity and to obtain access, typically a device that can be inserted in a door or a computer system.

(O'Reilly, 1992) (As cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS drafts Glossary of Terms Related to Information Security in Health Care Information Systems).

- **Treatment** – Means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
- **Unique user identifier** – A combination name/number assigned and maintained in security procedures for identifying and tracking individual user identify. (§142.308(c)(1)(v) HHS HIPAA Security NRPM)
- **Use** – Means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
- **User-based access** – Refers to a security mechanism used to grant users of a system access based upon the identity of the user.
- **User ID** – A unique identifier given to an individual allowing that individual access to a computer system. A User ID is usually accompanied by a password.
- **Workforce** – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

# Appendix B: Resources

## Disclaimer

The existence of a link or organizational reference in any of the following materials *should not* be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual Security and Privacy workgroup members. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by WEDI. The listing of an organization does not imply any sort of endorsement and WEDI takes no responsibility for the products, tools, and Internet sites listed.

Listed below are some valuable resources on the Internet that provide general information about HIPAA.

## Government Sites

The key HHS web site on HIPAA Administrative Simplification is called “Medical Privacy - National Standards to Protect the Privacy of Personal Health Information.” On this site, which the Office of Civil Rights maintains, you can find the December 28, 2000, Privacy Rule and its preamble, the August 14, 2002, modifications to the Privacy Rule, and its preamble, an integrated version of the Privacy Rule, and all other HHS guidance on the Privacy Rule which this resource document extensively references. You can email HHS questions about the Privacy Rule from this site. <http://www.hhs.gov/ocr/hipaa/>

HHS also maintains a general HIPAA Administrative Simplification site at <http://aspe.hhs.gov/admsimp/>.

The Centers for Medicare and Medicaid Services (CMS) offer a number of HIPAA related web sites:

- CMS HIPAA Site - <http://www.cms.hhs.gov/hipaa/hipaa2/default.asp>
- CMS’s Links to other Administrative Simplification Sites - <http://www.hcfa.gov/medicare/edi/hipaaedi.htm>
- CMS Internet Security Policy - <http://www.hcfa.gov/security/iseclply.htm>
- CMS Standards for Privacy of Individually Identifiable Health Information (Questions and Answers – July 2001) - <http://www.hhs.gov/ocdr/hipaa/finalmaster.html>

HHS’s National Committee on Vital and Health Statistics is the Secretary’s advisory body on HIPAA administrative simplification. [www.ncvhs.hhs.gov/](http://www.ncvhs.hhs.gov/)

Centers for Disease Control Public Health Data Standards Consortium - <http://www.cdc.gov/nchs/otheract/phdsc/phdsc.htm>

The Privacy Rule’s administrative requirements are similar to the compliance program requirements established in Chapter 8 of the Federal Sentencing Guidelines (<http://www.ussc.gov/2001guid/TABCON01.htm>) and the HHS OIG’s Compliance Program Guidance (<http://oig.hhs.gov/fraud/complianceguidance.html#1>). If your organization has developed either of these programs, that experience will be valuable in developing the HIPAA mandated policies and procedures. Even if it has not, understanding these compliance program requirements may provide valuable assistance in the HIPAA process.

The Government's Plain Language Action Network [www.plainlanguage.gov/](http://www.plainlanguage.gov/) will help your organization prepare a notice of privacy practices in plain language.

## **Association Sites**

Workgroup for Electronic Data Interchange (WEDI) – This not-for-profit association fosters widespread support for the adoption of electronic commerce in healthcare. [www.wedi.org](http://www.wedi.org)

Strategic National Implementation Process (SNIP) – A WEDI sponsored collaborative healthcare industry process for the development and implementation of standards. Site includes white papers on transactions, security, and privacy, such as this one. [snip.wedi.org](http://snip.wedi.org) SNIP has developed a walk around evaluation sheet. [http://snip.wedi.org/public/articles/HIPAA\\_Tour\\_Cklist1.pdf](http://snip.wedi.org/public/articles/HIPAA_Tour_Cklist1.pdf)

American Health Information Management Association (AHIMA) - <http://www.ahima.org/> This website has sample privacy forms for consent, authorization and notice of privacy practice.

CPRI – [www.cpri-host.org/resource/toolkit/toolkit.html](http://www.cpri-host.org/resource/toolkit/toolkit.html) This toolkit was devised by a consolidation of efforts from CPRI (Computer-based Patient Record Institute) and HOST (Healthcare Open Systems and Trials). The toolkit outlines best practices and examples of how to protect electronic and paper-based records

The Health Privacy Project of Georgetown University is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level. <http://www.healthprivacy.org/>

National Information Center for Health Services Administration [www.nichsa.org/](http://www.nichsa.org/)

National Uniform Claim Committee Administrative Simplification Links - <http://www.nucc.org/links/index.html>

# APPENDIX C: Use and Disclosures - Consent

Revision Date: 9/06/2002

## General Standard

Consent for Uses and Disclosures to carry out Treatment, Payment and Health Care Operation is no longer required by Federal Law (§164.506). However, State Law may require Consent. In that case, State Law Consent should be followed. It is required by the HIPAA Privacy Rule that the rendering provider is required to give the patient a copy of the provider's Notice of Privacy Practices and obtain a written acknowledgement of receipt from the individual. If a provider so chooses to obtain a Consent form, it is recommended to design one form to include both the Consent and the Acknowledgment of receipt of the Notice of Privacy Practices. (Check State Law on consent)

The text that follows was derived from the HIPAA Privacy Rule prior to the Modified Final HIPAA Privacy Rule. The guidelines may be used if a provider chooses to use the Consent. It is imperative, that if your State requires Consent, that the State Laws on Consent are followed, in addition with Federal Law requiring the acknowledgement of the Privacy Notice §164.520.

## **Citations**

The following sections of the final Privacy Rule and its preamble discuss issues related to obtaining consent for the use and disclosure of an individual's protected health information.

- §164.502(a)(1) – Permitted Uses and Disclosures
- §164.506 – Consent for Uses and Disclosures to Carry out Treatment, Payment and Health Care Operations
- §164.510 – Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object
- §164.512 – Uses and Disclosures for which Consent, Authorization or Opportunity to Agree or Object is not Required
- §164.532 – Transition Provisions
- Preamble, pg. 82509 – 15 – Discussion of Consent
- Preamble, pg. 82649 – 50 – Discussion of Consent

## **General Requirements**

### Details of Standard:

**Exceptions:** Exceptions to the consent requirement permit use and disclosure without consent:

- In emergency treatment situations, if the provider *attempts* to obtain consent as soon as reasonably practicable after the delivery of such treatment;
- If the provider is under a legal obligation to treat the individual, attempts to obtain such consent, but is unable to do so; or

If a provider attempts to obtain consent, is unable to do so because of substantial communication barriers, but determines, in the exercise of professional judgment, that consent to receive treatment may be clearly inferred from the circumstances.

A provider that provides treatment after having unsuccessfully attempted to obtain consent must document its attempt and the reason it proved unsuccessful.

**Miscellaneous:** Covered entities other than health care providers with a direct patient relationship *may* seek consents for their own purposes; but, if they do so, such consents must comply with the requirements for consents applicable to health care providers with a direct patient relationship. If a covered entity that is not required to obtain consent seeks to obtain one and the individual refuses to execute it, the covered entity may not use or disclose the protected health information for any of the purposes contained in the consent.

Except in the case of joint consents for organized health care arrangements, a consent obtained by one covered entity is not effective to permit another covered entity to use or disclose protected health information, unless the other covered entity is functioning as a business associate. [The Supplementary Information published with the final regulation takes the position that when a covered entity is acting as a business associate of another covered entity, its actions for or on behalf of the principal covered entity are authorized by the consent obtained by the principal covered entity.]

Consent does not permit a use or disclosure of protected health information when an authorization is required.

## **Policies and Procedures**

In order to put into place the implementation specifications relating to consent, a covered entity needs to develop policies and procedures regarding each of the following implementation specifications:

### **Conditioning services on obtaining consent**

A health care provider may condition treatment, and a health plan may condition enrollment, on the individual providing the consent required by the rule. However, the health plan must seek the consent at the time of enrollment, and a health plan may not condition the provision of any services on obtaining consent if consent is sought after enrollment.

### **Combining consents with other documents**

If a Covered Healthcare Provider chooses to utilize the Consent Form it is recommended to design one form to include both Consent and the Acknowledgement of Receipt of Notice of Privacy Practices. However, if State Law requires Consent, the State Law of Consent rules must be applied. Consent for use or disclosure may also be combined with a research authorization.

### **Revocation of consents:**

An individual may revoke consent at any time, except to the extent that the covered entity has taken action in reliance thereon. Any revocation must be in writing. Upon receipt of a revocation of consent, a health care provider may discontinue treatment and a health plan may disenroll an individual.

### **Content of Consent Form**

A consent form must:

- 1) Be in plain language;
- 2) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment, or health care operations;
- 3) Refer the individual to the entity's Notice of Privacy Practices and state that the individual has the right to review the notice prior to signing the consent. An acknowledgement of the Notice of Privacy must be signed and a copy recorded. If allowed by State Law, this may be combined on one form.
- 4) If the covered entity has reserved the right to change the privacy practices described in the notice, state that the terms of the notice may change and describe how the individual may obtain a revised notice;
- 5) State that:
  - a) 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;
  - b) The covered entity is not required to agree to requested restrictions; and
  - c) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;
- 6) Inform the individual of his or her right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and
- 7) Be signed and dated by the individual.

Consents must convey that the covered entity may use or disclose protected health information for its own treatment payment and operations. The covered entity may disclose PHI to another covered entity for treatment, payment or operations or for fraud and abuse detection or compliance. Consents must also include if the covered entity participates in an organized health care arrangement.

### **Defective Consents**

A consent that lacks any of the elements described under "Implementation Specifications: Content" is void and of no effect, as is any consent that has been revoked.

### **Resolving Conflicting Consents and Authorizations**

If a covered entity is in possession of two or more consents (or other authorization or written legal permission) from an individual regarding disclosure of protected health information to carry out treatment, payment, or health care operations, the covered entity must act in accordance with the most restrictive. Alternatively, it may attempt to resolve the conflict by obtaining a new consent that complies with the requirements of the Privacy Rule or by determining the individual's preferred resolution of the conflict through oral or written communication with the individual. The preferred resolution of the individual must be documented and followed.

### **Joint Consent Requirements**

Covered entities that participate in an organized health care arrangement and that have a joint Notice of Privacy Practices may utilize a single document that provides the requisite consent to all the covered entities in the organized health care arrangement.

A joint consent must include the names or other specific identification of the covered entities to which the joint consent applies and otherwise comply with the regulation's requirements regarding consents, except that content may be altered to reflect that the consent covers more than one entity.

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.

### **Differences Between a Consent and an Authorization**

The Supplementary Information published with the final Privacy Rule makes clear that consent and an authorization differ both in the circumstances in which they are required and in content.

### **No Waiver of Privilege Available Under Law**

The Supplementary Information published with the final Privacy Rule notes that the act of executing a consent should not be construed to waive, directly or indirectly, any privilege granted under federal, state, or local law or procedure.

### **Scope of Consent**

The Supplementary Information published with the final Privacy Rule indicates that the covered entity must make the decision as to what uses and disclosures of protected health information it will make and obtain consent for all such uses and disclosures. However, a covered entity is not required to obtain consent to use or make disclosures of protected health information if the covered entity does not intend to (and does not) make such use or disclosure of protected health information.

### **Consent Signature**

Once the proposed standards regarding electronic signatures have been finalized, a signature in compliance with those regulations will suffice for consent purposes. No independent verification of the authenticity of a signature on a consent form, or the signer's identity, is affirmatively required. However, it is expected that the same level of scrutiny will be observed, as is the case when a provider obtains the individual's consent to undergo treatment.

### **Other Consent References**

Consent is part of and integral to other major topics of the Privacy regulations. Rather than include the volumes of information from those topics, this paper includes them by reference. The other topics are:

- §164.510 – Uses and Disclosures requiring an opportunity for the individual to agree or object
- §164.512 – Uses and Disclosures requiring for which consent, authorization, or opportunity to agree or object is not required
- §164.532 – Transition Provisions

# Acknowledgements

WEDI/SNIP would like to express its appreciation to the authors and reviewers for their efforts preparing this White Paper.

Jana Aagaard

Paula Anderson

Eric Arnett, Jewish Home for the Elderly of Fairfield

Mary Bennett, Ethical Leadership Group

Karen Blackwell, U. of Kansas Medical Center

Joan Boyle, The TriZetto Group, Inc.

Lisa R. Cavitt, Southern Illinois Healthcare

Noel Chang, Integral Practice Solutions

Steve Chevalier, Senior Consultant, Daou-RHI

John R. Christiansen Preston | Gates | Ellis LLP

Rose Cintron-Allen, Teradata, a division of NCR

Pat Cross

Rachel Dalthorp, U. of Kansas Medical Center

Ping Ma Dixon, The TriZetto Group, Inc.

David M. Ermer, Gordon & Barnett

Mike Falzano, The TriZetto Group, Inc

Boulton Fernando, Ernst & Young

Scot Ferrell, Ernst & Young

Hope Furtado, TM Floyd & Co., Inc.

Peter B. Goldstein, Esq., Cap Gemini Ernst & Young

Kathleen Graham, Children's Health System,  
Birmingham, Alabama

Pamela Garay, Affiliated Computer Services, Inc .

Louise R. Gregg, IV-Chenango, Delaware, Otsego,  
and Schoharie Counties Community Services, New  
York

Leslie Harpe, South Georgia Medical Center

Janet Hillock Barone, HealthTrio

Vickie Hohner, Washington St. Dept. of Health

Christine Jensen, Denver Health

Lester Jones, Ph.D., JAMMS

Paul Kelley, MediQual Systems, Inc.

Laura Kedrick

Ken Kirch, KPMG LLP

Laura Lynn Kerner, Recall Systems

M.Beth Kranda, Affiliated Computer Services, Inc .

Pat Lareau, Lareau & Associates

Peter Lareau, Lareau & Associates

Scott Last, Anthem Insurance Inc.

James H. Leigh, Jr. MD: The Longstreet Clinic

Dawn Lenox, North Oaks Health System

Jerry Malooley Healthcare Solutions

Christopher M. Mangelli, JD, U of S. Maine

Jonathon May, HuTech Resources

Julie McCarter Great-West Life

Tim McGuinness, Ph.D.HIPAA Conformance  
Certification Organization (HCCO)

Dale Meyers

Wayne J. Miller, Esq., Reish Luftman McDaniel &  
Reicher

Patricia Y. Miller, Esq., Reish Luftman McDaniel &  
Reicher

Lisa T. Murphy, Miller & Chevalier

Todd Nebeker, The TriZetto Group, Inc.

Kevin Olson, Great Plains Medical Center

Albert Oriol, The Children's Hospital, Denver

Kimiko Orosz., Hazen Group, Inc.

Jeri Ostling, Teradata, a division of NCR

Linda Owings, Tillinghast

Donna Padnos, Superior Consultant

Kimberly Patton

Joseph Poisson, Keane, Inc.

Jennifer Proko RN, Health Care Savings

John R. Christiansen Preston | Gates | Ellis LLP

Matthew Randolph, Ernst & Young

Becky Reed, Alera Solutions

Pam Stone, Collective Solutions, Inc.  
Trish Savitsky, Blue Cross of N.E. Pennsylvania  
Rebekah Savoie, Smith, Turner & Reeves  
Payal Shirvaikar, American Management Systems, Inc  
Connie Stephenson, The TriZetto Group, Inc.  
Maria Stolze, Parkview Health  
Michael Thoni, Superior Consultant  
Jacob Vishnevsky, Stelex-TVG, Inc.  
LuAnn Weis, HealthCare Solutions of NJ  
Christine Williams, Gordon, Feinblatt  
Ken Yale, Eduneering

**Privacy Policies & Procedures Modifications**  
**Update Sub-Workgroup Leaders:**

Noel Chang, Integral Practice Solutions  
David M. Ermer, Gordon & Barnett  
James H. Leigh, Jr. MD: The Longstreet Clinic  
Christine Williams, Gordon, Feinblatt  
Ken Yale, Eduneering

**Privacy Policies & Procedures Co-Chairs**

Joan Boyle, The TriZetto Group, Inc.  
M. Beth Kranda, Affiliated Computer Services, Inc .  
Scott Last, Anthem Insurance, Inc.

# Privacy Policies & Procedures Checklist

	Topic	Note	P&P Development Team	Start Date/ Completion Date	Status	Comments
	General					
	Organizational Requirements – an Overview	1				
	Organizational Requirements: Affiliated Covered Entities	1				
	Business Associates	1				
	Organizational Requirements: Group Health Plans	3				
	Organizational Requirements: Hybrid Entities	1				
	Organizational Requirements – Organized Health Care Arrangements	2				
	Preemption of State Law	1				
	Administrative Requirements					
	Changes in Law	1				
	Complaint Process	1				
	Designation of Privacy Officer and Contact Person/Office	1				
	Documentation	1				
	Mitigation	1				
	Safeguards: Administrative, Technical and Physical	1				
	Sanctions against Staff Members	1				

Topic	Note	P&P Development Team	Start Date/ Completion Date	Status	Comments
Training for Staff	1				
Whistleblowers	1				
Individual's Rights					
Accounting for Disclosures	1				
Inspect and Copy	1				
Notice of Privacy Practices	1				
Request Amendment	1				
Request Confidential Communication	1				
Request Restriction of Disclosures	1				
Permissible Uses and Disclosures					
Authorizations	1				
Communications with Brokers and Agents	3				
Consent Requirement <b>NOTE:</b> Consent forms are not required by HIPAA, They may be required by State law or Entities may elect to use them.	2				
Deceased Individuals	1				
De-identification of protected health information	1				
Emergency Situations	2				
Employer/ Plan Sponsor	3				

	<b>Topic</b>	<b>Note</b>	<b>P&amp;P Development Team</b>	<b>Start Date/ Completion Date</b>	<b>Status</b>	<b>Comments</b>
	Marketing and Fundraising	1				
	(Miscellaneous ) Permitted without an Authorization or Allowing the Individual and Opportunity to Object	1				
	Minimum Necessary	1				
	Permitted Under the Privacy Rule	1				
	Personal Representatives	1				
	Required by Law	1				
	Requiring an Opportunity for the Individual to Agree or Object	1				
	Research Activities	2				
	Underwriting and Related Purposes	3				
	Verification of identity	1				
	Victims of Abuse, Neglect, Domestic Violence and Crime	1				
Note 1 -- Topic is of general interest to all covered entities						
Note 2 -- Topic is principally of interest to covered entities that are health care providers						
Note 3 -- Topic is principally of interest to covered entities that are health plans						