HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES

ICN 909001 August 2016

Please Note:

The information in this publication applies to HIPAA covered entities, which include most health care professionals and health care organizations, as well as their business associates. When "you" is used in this publication, we are referring to these persons and entities.

Table 2. Hyperlink Table, at the end of this document, provides the complete URL for each hyperlink.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and provide individuals with certain rights to their health information. This publication discusses:

- The **Privacy Rule**, which sets national standards for when protected health information (PHI) may be used and disclosed
- The **Security Rule**, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)
- The **Breach Notification Rule**, which requires covered entities to notify affected individuals, U.S. Department of Health & Human Services (HHS), and in some cases, the media of a breach of unsecured PHI

You play a vital role in protecting the privacy and security of patient information. This publication gives an overview of the rules, and it outlines the information protected by and who must comply with those rules.

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes standards for the protection of PHI held by:

- Health plans
- Health care clearinghouses
- Those health care providers that conduct certain health care transactions electronically
- Their business associates

The Privacy Rule gives patients important rights with respect to their health information, including rights to examine and obtain a copy of their health records in the form and manner they request, and to ask for corrections to their information. Also, the Privacy Rule permits the use and disclosure of health information needed for patient care and other important purposes.

Protected Health Information

The Privacy Rule protects individually identifiable health information, called PHI, held or transmitted by a covered entity or its business associate, in any form, whether electronic, paper, or verbal. PHI includes information that relates to all of the following:

- The individual's past, present, or future physical or mental health or condition
- The provision of health care to the individual
- The past, present, or future payment for the provision of health care to the individual

PHI includes many common identifiers, such as name, address, birth date, and Social Security number.

Visit the HHS HIPAA Privacy Rule webpage for more information.

HIPAA Security Rule

The HIPAA Security Rule specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of ePHI.

Covered entities and business associates must develop and implement policies and procedures to protect the security of ePHI they create, receive, maintain, or transmit. Each entity must analyze the risks to ePHI in its environment and create solutions appropriate for its own situation. What is reasonable and appropriate depends on the nature of the entity's business, as well as its size, complexity, and resources. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the ePHI
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce

HIPAA Security Rule (Cont.)

Confidentiality: ePHI is not available or disclosed to unauthorized people

Integrity: ePHI is not altered or destroyed in an unauthorized manner

Availability: ePHI is accessible and usable on demand by an authorized person

The Security Rule does not dictate security measures but requires covered entities to consider all of the following:

- Size, complexity, and capabilities
- Technical, hardware, and software infrastructure
- The costs of security measures
- The likelihood and possible impact of risks to ePHI

Covered entities must review and modify security measures to continue protecting ePHI in a changing environment.

Visit the HHS HIPAA Security Rule webpage for more information.

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, HHS, and in some cases, the media of a breach of unsecured PHI. Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach. Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to HHS annually. The Breach Notification Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.

Visit the HHS HIPAA Breach Notification Rule webpage for more information and guidance on the reporting requirements.

Who Must Comply With HIPAA Rules?

Covered entities and business associates, as applicable, must follow HIPAA rules. If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA rules. For a complete definition of a covered entity and a business associate, refer to the "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification" Final Rule.

Covered Entities

Covered entities electronically transmit health information. The following covered entities must follow HIPAA standards and requirements:

Covered Health Care Provider: Any provider of medical or other health care services or supplies who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard, such as:

- Chiropractors
- Clinics
- Dentists
- Doctors
- Nursing homes
- Pharmacies
- Psychologists

Covered Entities (Cont.)

Health Plan: Any individual or group plan that provides or pays the cost of health care, such as:

- Company health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs
- Health insurance companies
- Health maintenance organizations (HMOs)

Health Care Clearinghouse: A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice versa, such as:

- Billing services
- Community health management information systems
- Repricing companies
- Value-added networks

Business Associates

A business associate is a person or organization, other than an employee of a covered entity, that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI. A business associate can also be a subcontractor responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate. Business associates provide services to covered entities that include:

- Accreditation
- Billing
- Claims processing
- Consulting
- Data analysis
- Financial services
- Legal services
- Management administration
- Utilization review

Business Associates (Cont.)

NOTE: A covered entity can be a business associate of another covered entity.

If a covered entity enlists the help of a business associate, then a written contract or other arrangement between the two must:

- Detail the uses and disclosures of PHI the business associate may make
- Require that the business associate safeguard the PHI

Visit the HHS HIPAA Covered Entities and Business Associates webpage for more information.

Enforcement

The HHS Office for Civil Rights enforces the HIPAA Privacy, Security, and Breach Notification Rules. Violations may result in civil monetary penalties. In some cases, criminal penalties enforced by the U.S. Department of Justice may apply.

Common noncompliance issues include:

- Impermissible PHI uses and disclosures
- Lack of PHI safeguards
- Lack of patients' access to their PHI
- Use or disclosure of more than the minimum necessary PHI
- Lack of administrative ePHI safeguards

Enforcement (Cont.)

The following are actual case examples:

- **Settlement**: Two covered entities inadvertently posted ePHI for 6,800 individuals on the web, including patient status, vital signs, medications, and laboratory results. The investigation found that neither entity made efforts to assure the security of the server hosting the ePHI or confirm it contained adequate software protections. Neither entity developed an adequate risk management plan that addressed potential threats and hazards to ePHI. The entities agreed to pay a combined settlement of $4.8 million and enter into corrective action plans.
- **Criminal prosecution**: A former hospital employee pleaded guilty to criminal HIPAA charges after obtaining PHI with the intent to use it for personal gain. He faced up to 10 years in prison.

Visit the HHS HIPAA Compliance and Enforcement webpage for more information.

Resources

The Centers for Medicare & Medicaid Services (CMS) HIPAA Privacy and Security Information webpage provides more information, or you may refer to the resources listed in Table 1.

Table 1. HIPAA Privacy, Security, and Breach Notification Resources

Resources	Website
Are You a Covered Entity?	CMS.gov/Regulations-and-Guidance/AdministrativeSimplification/HIPAA-ACA/AreYouaCoveredEntity.html
Business Associate Contracts	HHS.gov/hipaa/for-professionals/covered-entities/ sample-business-associate-agreement-provisions
Business Associate Frequently Asked Questions	HHS.gov/hipaa/for-professionals/faq/businessassociates
"Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care"	HHS.gov/sites/default/files/provider_ffg.pdf
Disclosures in Emergency Situations	HHS.gov/hipaa/for-professionals/special-topics/emergency-preparedness
Fast Facts for Covered Entities	HHS.gov/hipaa/for-professionals/covered-entities/fast-facts

Resources (Cont.)

Table 1. HIPAA Privacy, Security, and Breach Notification Resources (Cont.)

Resources	Website
"Frequently Asked Questions About the Disposal of Protected Health Information"	HHS.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf
HealthIT.gov Privacy and Security	HealthIT.gov/providers-professionals/ehr-privacy-security
Model Notices of Privacy Practices	HHS.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices
"Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification" Final Rule	GPO.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
Security Rule Guidance Material	HHS.gov/hipaa/for-professionals/security/guidance
Training Materials	HHS.gov/hipaa/for-professionals/training

Resources (Cont.)

Table 2. Hyperlink Table

Resources	Website
HIPAA Breach Notification Rule	http://www.hhs.gov/hipaa/for-professionals/breach-notification
HIPAA Compliance and Enforcement	http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement
HIPAA Covered Entities and Business Associates	http://www.hhs.gov/hipaa/for-professionals/covered-entities
HIPAA Privacy and Security Information	https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/PrivacyandSecurityInformation.html
HIPAA Privacy Rule	http://www.hhs.gov/hipaa/for-professionals/privacy
HIPAA Security Rule	http://www.hhs.gov/hipaa/for-professionals/security
Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification	https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf