



## THE HIPAA PRIVACY RULE AS A FOUNDATION FOR ELECTRONIC HEALTH INFORMATION EXCHANGE

The *Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule”) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals’ privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

The Privacy Rule applies to health plans, health care clearinghouses, and those health care providers who conduct electronically certain financial and administrative transactions that are subject to the transactions standards adopted by HHS.

The Privacy Rule requires covered entities to protect individuals’ health records and other identifiable health information by requiring appropriate safeguards to protect privacy, and by setting limits and conditions on the uses and disclosures that may be made of such information. The Privacy Rule also gives individuals certain rights with respect to their health information. The Privacy Rule provides a strong foundation for developing electronic health information exchange relationships and business models. Its underlying policies and provisions reflect the careful balance between protecting the privacy of individuals’ PHI (Protected Health Information) and assuring that such health information is available to those who need access to it to provide health care, payment for care, and for other important purposes. The Privacy Rule’s provisions also provide considerable flexibility to accommodate covered entities’ utilization of Health Information Organizations (HIOs) and networked environments.

In that regard, the Privacy Rule expressly permits a covered entity to disclose PHI to a business associate, or allow a business associate to create or receive PHI on its behalf, so long as the covered entity obtains satisfactory assurances in the form of a contract or other agreement that the business associate will appropriately safeguard the information.

A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

**Organizations that have to follow** the Privacy Rule include:

- Health plans
- Health care clearinghouses
- Health care providers who conduct electronically certain financial and administrative transactions that are subject to the transactions standards adopted by HHS
- Business Associates (see definition below)

**9800 Bren Rd East, Suite 400, Minnetonka, MN 55343  
(952) 893- 2030 or 1- 877- 755-2030  
[www.phenomenalnetworks.com](http://www.phenomenalnetworks.com)**



**Examples of organizations that do not have to follow the Privacy Rule include:**

- life insurers,
- employers
- workers compensation carriers,
- many schools and school districts,
- many state agencies like child protective service agencies,
- many law enforcement agencies,
- many municipal offices.

### **What Information Is Protected**

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's computer system
- Billing information about you at your clinic
- Most other health information about you held by those who must follow this law

### **Business Associates**

**Business Associate Defined.** In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing. Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity.

**Business Associate Contract.** When a covered entity uses a contractor or other non-workforce member to perform "*business associate*" services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates. Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Rule.



## Protected Health Information.

The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

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

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C.

## Limiting Uses and Disclosures to the Minimum Necessary

**Minimum Necessary.** A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

**Access and Uses.** For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.



**Disclosures and Requests for Disclosures.** Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures*, that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria.

**Reasonable Reliance.** If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation

### **General steps for HIPAA Compliance**

- Identify all information systems that house EPHI (Electronic Protected Health Information)
- Include all hardware and software that are used to collect, store, process, or transmit EPHI.
- Analyze business functions and verify ownership and control of information system elements as necessary.

### **Enforcement and Penalties for Noncompliance**

**Compliance.** The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes a set of national standards for the use and disclosure of an individual's health information – called protected health information – by covered entities, as well as standards for providing individuals with privacy rights to understand and control how their health information is used. The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for administering and enforcing these standards and may conduct complaint investigations and compliance reviews.

Consistent with the principles for achieving compliance provided in the Privacy Rule, OCR will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Privacy Rule. Covered entities that fail to comply voluntarily with the standards may be subject to civil money penalties. In addition, certain violations of the Privacy Rule may be subject to criminal prosecution. These penalty provisions are explained below.



**Civil Money Penalties.** OCR may impose a penalty on a covered entity for a failure to comply with a requirement of the Privacy Rule. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

	<b>For violations occurring prior to 2/18/2009</b>	<b>For violations occurring on or after 2/18/2009</b>
<b>Penalty Amount</b>	Up to \$100  per violation	\$100 to \$50,000 or more  per violation
<b>Calendar Year Cap</b>	\$25,000	\$1,500,000

## STATE LAW

**Preemption.** In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply. "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.

For more information and updates

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>