HIPAA

Lesson 2. The HIPAA Privacy Rule

Prepared By: Lucas Dominic Fuentes Balaguer

ONQ

HIPAA Privacy Rule

The Privacy Rule establishes national standards for the protection of certain health information. The Privacy Rule standards address the use and disclosure of PHI as well as standards for individuals' privacy rights to understand and control how their health information is used and shared, including rights to examine and obtain a copy of their health records as well as to request corrections.

The imposition of civil and criminal penalties is possible for violations of HIPAA and the HIPAA Privacy Rule. ***This rule protects the PHI in any format: written, spoken, or electronic***.

Patient's Rights

- ***Right to access and receive a copy of one's own PHI*** (paper or electronic formats).
- Right to request amendments to information.
- Right to request restriction of PHI uses and disclosures.
- Right to restrict disclosure to health plans for services self-paid in full ("self-pay restriction").
- ***Right to Confidential Communications***.
- Right to request alternative forms of communications (mail to P.O. Box not street address; no message on answering machine, etc.).
- Right to an accounting of the disclosures of PHI.

Notice of Privacy Practices (NPP)

Covered entities must prominently post and distribute a Notice of Privacy Practices (NPP). ***The notice must describe the ways in which the covered entity may use and disclose PHI***. The notice must state the covered entity's duties to protect privacy, provide an NPP, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to the U.S. Department of Health and Human Services (HHS) and to the CE if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices.

The Rule also contains specific distribution requirements for health care providers and health plans.

Content of the NPP

The NPP must include the following information:

- How the covered entity may use and disclose an individual's PHI.
- ***The individual's rights with respect to the information and how the individual may exercise these rights***, including how the individual may complain to the covered entity.
- The covered entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of PHI.
- Whom individuals can contact for further information about the covered entity's privacy policies.

Treatment, Payment and Operations: The "TPO" Rule

Covered entities may use and disclose PHI for **treatment**, **payment**, and health care **operations activities** — and other permissible or required purposes consistent with the HIPAA Privacy Rule — *without* obtaining a patient's written permission (consent or authorization).

TPO includes teaching, medical staff/peer review, legal, auditing, quality reviews, **customer service**, **business management**, and releases mandated by law.

Covered entities must have a **Business Associate Agreement** (BAA) regarding to the access or use of PHI when providing a service to the entity.

Examples of TPO

- The patient's referring physician calls and asks for a copy of the patient's recent exam at a specific facility (Treatment).
- A patient's insurance company calls and requests a copy of the patient's medical record for a specific service date (Payment).
- The Quality Improvement office calls and asks for a copy of an Operative Report (Health Care Operations).

REMEMBER: Only for TPO purposes, the patient's information can be provided.

Purposes Other Than TPO

Unless required or permitted by law, there must be a **written authorization** from the patient to access, use or disclose their information.

- **Patient's Authorization** allows to disclose information for purposes not related to treatment, payment, or operations (TPO).

REMEMBER: *Apart from TPO, the PHI may not be accessed, used or disclosed without a HIPAA Authorization.*

The Minimum Necessary Standard

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

Except for disclosures to other health care providers for treatment purposes, ***the covered entity must make reasonable efforts to use or disclose only the minimum amount of PHI needed to accomplish the intended purpose of the use or disclosure*** (the minimum necessary standard).

When this minimum necessary standard applies to a use or disclosure, the covered entity may not use or disclose the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

ONQ

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, the United States Department of Health and Human Services(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.

Notification by a Business Associate

If a business associate is responsible for a breach of unsecured PHI, the business associate must notify the covered entity and provide the information necessary to permit the covered entity to provide the required notice. Notice must be provided without unreasonable delay, and **in no case later than 60 calendar days after discovery of the breach**.

Covered entities will need to negotiate with their business associates regarding the time frame and manner in which a business associate will notify the covered entity of the breach, and incorporate such information into their business associate agreements.

ONQ

Important Things To Remember

- The HIPAA Privacy Rule ***protects the PHI in any format: written, spoken, or electronic***.
- Two of the most important patient rights stablished by the ***Privacy Rule*** are: ***Right to access and receive a copy of one's own PHI*** and the ***Right to Confidential Communications***.
- Unless it is for TPO purposes, ***the PHI may not be accessed, used or disclosed without a HIPAA Authorization***.
- ***The Minimum Necessary Standard permits to use or disclose only the minimum amount of PHI needed*** to accomplish the intended purpose of the use or disclosure.
- The Breach Notification Rule requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.

HIPAA

Health Insurance Portability and Accountability Act

Thanks!