HIPAA Privacy and Security Rules: A Refresher

Marilyn Freeman, RHIA
California Area HIPAA Coordinator
California Area HIM Consultant

Objectives

- Provide overview of Health insurance Portability and Accountability Act (HIPAA)
- Discuss the Privacy Rule and its purpose
- Identify when private information can or cannot be disclosed
- Explain how HIPAA and the Privacy Rule affect public health

Acronyms

Term	Meaning
BA	Business Associate
BAA	Business Associate Agreement
CE	Covered Entity
EHR	Electronic Health Record
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
MU	Meaningful Use
NPP	Notice of Privacy Practices
TPO	Treatment, Payment, and Operations

What is HIPAA

- The Health Insurance Portability and Accountability Act was enacted in 1996
- HIPAA became effective in 2004 and consisted of THREE rules:
  - Privacy
  - Security
  - Code Sets and Transactions
- The HITECH (Omnibus) Final Rule reinforced security requirements and added breach notification requirements

Defining the Rules

- **Privacy Rule** protects the privacy of individually identifiable health information
- **Security Rule** sets national standards for the security of electronic protected health information (ePHI)
- **Breach Notification Rule** requires covered entities and business associates to

Why Do Privacy and Security Matter?

- Providers and patients must trust that an individual’s health information is private and secure
- If patients lack trust in the electronic health record (EHR) and health information exchanges (HIE), they may not want to disclose health information
- If patients withhold health information, there could be life-threatening consequences

Cultivating Patient Trust

- Maintain accurate information in patient's records
- Make sure patients have a way to request electronic access to their medical record…and know how to do so
- Carefully handle patient's health information to protect their privacy
- Ensure patients' health information is accessible to authorized representative when needed

What is Protected?

Individually identifiable health information is information (including demographic info) 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.

Elements of PHI

- Names
- All geographic subdivisions smaller than a State
- All elements of dates (except year) for dates directly related to an individual
- 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 (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code;

HIPAA Notice of Privacy Practices (NPP)

Must describe the ways in which the provider may use and disclose protected health information (PHI)

1. Provide to patients at first visit
2. Post prominently in clinic and on website
3. Provide to any patient upon request

Should I follow HIPAA or State Law?

- Always follow the most stringent requirement
- HIPAA is intended to be a “floor” or minimum requirement
- State requirements “trump” HIPAA when they are stricter

When is patient consent required?

- A covered entity (CE) may use and disclose PHI for its own treatment, payment, and health care operations activities without the patient's written consent
- A covered entity may also disclose PHI for treatment, payment, and health care operations activities when both CE's have a relationship with the patient, the PHI pertains to the relationship, the data requested is minimum necessary
- Treatment, Payment, Operations (TPO) include quality assessment or improvement, review of quality or competence of health professionals, fraud and abuse detection or compliance

What is a Breach?

- A breach is, generally, an **impermissible use or discl**osure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is **presumed to be a breach** unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the protected health information or to whom the disclosure was made;
  - Whether the protected health information was actually acquired or viewed; and
  - The extent to which the risk to the protected health information has been mitigated.

Incident Reporting Requirements

- Clinic – Employees must report a privacy INCIDENT
  - To Immediate Supervisor
  - Privacy Officer

Facility Breach Reporting Requirements

If the privacy incident is determined to be a BREACH, it must be reported. Federal and State requirements vary. It is important to comply with both.

- Federal
  - A covered entity must notify the Secretary (DHHS) if it discovers a breach of unsecured protected health information. (See 45 C.F.R. § 164.408)
- California
  - Report to the California Department of Public Health within 5 business days of detection (See California Health and Safety Code Section 1280)
  - In some cases, report is required to the California Attorney General (See California Civil Code Section 1798.82)

Resources

- “Guide to Privacy and Security of Electronic Health Information” Version 2.0, April 2015, The Office of the National Coordinator for Health Information Technology http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- HIPAA Breach Notification Rule http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
- California Breach Reporting

  http://www.ohi.ca.gov/calohi/ohii-medical-privacy-breach-reporting.htm

Marilyn Freeman, RHIA

marilyn.freeman@ihs.gov

Office: 916 930-3981 X362

Mobile: 916 716-1908