HIPAA: Breach Notification

By: Office of University Counsel

For: Jefferson IRB Continuing Education

September 2014

Introduction

- **The HIPAA Privacy Rule establishes the conditions under which Covered Entities can provide researchers access to and use of protected health information for research purposes.**
- **The HIPAA Privacy Rule does not replace or act in lieu of other federal regulations such as HHS Protection of Human Subjects and the FDA Protection of Human Subjects.**

HIPAA Privacy Rule

- **Covered Entity** is a health plan, a health care provider or a health care clearinghouse that electronically transmits any health information in connection with transactions for which HHS has adopted standards.
- **Protected Health Information (PHI):**
  - Relates to past, present, or future physical or mental condition of an individual; provisions of healthcare to an individual; or for payment of care provided to an individual.
  - Is transmitted or maintained in any form (electronic, paper, or oral representation).
  - Identifies, or can be used to identify the individual.

HIPAA Security Rule

- The **Security Rule** defines the standards which require covered entities to implement basic safeguards to protect electronic PHI (e-PHI).
- **e-PHI** (electronic Protected Health Information) is computer-based patient health information that is **used, created, stored, received or transmitted** by a Covered Entity using any type of electronic information resource.

How Can Covered Entities Use and Disclose PHI for Research and Comply with the HIPAA Privacy Rule?

- **PHI may be used and disclosed for research WITH an individual's written permission in the form of an Authorization (OHR-B Informed Consent Form)**
- **PHI may be used and disclosed for research WITHOUT an Authorization in limited circumstances: (a) under a waiver of the Authorization requirement; (b) for research on decedents' information; (c) preparatory to research; and (d) as a limited data set with a data use agreement**

Protection of PHI

- **Example: The IRB may waive Authorization upon the request of a researcher only if the use or disclosure of PHI involves not more than a minimal risk to the privacy of individuals, based on:**
  - **An adequate plan to protect the identifiers**
  - **A plan to destroy identifiers as soon as possible**
  - **Adequate written assurances that the PHI will not be reused or disclosed to any other person**
- **Researchers must provide a plan to protect PHI and implement that plan**

HITECH-Breach Notification Provisions

- **The HITECH Act applies to breaches of "unsecured protected health information"**
- **Information must be encrypted or destroyed in order to be considered "secured"**

HITECH-What Constitutes a Breach?

A "breach" is an impermissible acquisition, access, use or disclosure not permitted by the HIPAA Privacy Rule.

Examples include:

- **Laptop containing PHI is stolen**
- **Researcher who is not authorized to access PHI looks through patient files in order to learn of a person's treatment**
- **Researcher misplaces research documents with study subject PHI and social security number**
- **Researcher sends wrong sponsor study subject information including PHI**
- **Researcher sends sponsor more PHI than necessary**
- **Research office theft results in stolen PHI**

HITECH-Breach Notification Obligations

If a breach has occurred, a Covered Entity will be responsible for providing notice to:

- **The affected individuals (without unreasonable delay and in no event later than 60 days from the date of discovery)**
- **The Secretary of the U.S. Department of Health and Human Services (timing will depend on number of individuals affected by the breach)**
- **The media (only required if 500 or more individuals of any one state are affected)**

The OHR must consider reporting obligations.

Penalties for Violations

- A violation of federal regulations can result in civil money penalties or criminal penalties.
- Penalties can be imposed for underlying HIPAA Privacy Rule violation even if the breach is properly handled.

Civil Money Penalty Enhancement

- **Unknowing Violations:** $100 to $50,000 per violation
- **Negligent Violations:** $1,000 to $50,000 per violation
- **Willful Neglect: "Conscious intentional failure or reckless indifference to the obligation to comply"**
  - $10,000 to $50,000 per violation (if corrected within 30 days)
  - $50,000 per violation (if not corrected)

$1.5M cap per calendar year for all violations of the same type

Enforcement

$150,000 settlement with Adult & Pediatric Dermatology, P.C. of Concord, Massachusetts for loss of unencrypted flash drive and not having policies to address breach notification provisions.

Enforcement

$1,215,780 settlement with Affinity Health Plan for impermissibly disclosing PHI of 344,579 affected individuals when it returned multiple photocopiers to leasing agents without erasing the data on the copier hard drives.

Enforcement

$1,700,000 settlement with Well Point for security weaknesses in an online application database that left the e-PHI of 612,402 individuals accessible to unauthorized individuals over the Internet. The data included names, dates of birth, addresses, social security numbers, telephone numbers and health information.

Enforcement

- **$1.5M settlement with BCBS of TN over the loss of 57 hard drives containing 1M patient records**
- **$865,000 settlement with UCLA Medical Center after hospital employees allegedly accessed the records of two celebrity patients without authority**
- **$1M settlement with Mass General after employee left 192 HIV patients records on subway**

Enforcement

- **$50,000 settlement with Hospice of Northern Idaho after theft of laptop containing unencrypted PHI of 441 patients**
- **$1.5M settlement with Mass Eye & Ear after theft of laptop containing unencrypted PHI of 3,621 patients**
- **$1.7M settlement with Alaska DHHS after theft from employee's vehicle of USB hard drive possibly containing PHI**
- **$100,000 settlement with Phoenix Cardiac Surgery which posted clinical and surgical appointments in Internet-based calendar that was publicly available**

Jefferson
HEALTH IS ALL WE DO

Questions?