HIPAA Health Insurance Portability & Accountability Act

This presentation and materials provided are for informational purposes only. Please seek legal advisor assistance when dealing with privacy and security issues. Trinity materials are specific to Trinity Health entities and are not meant to serve as formal legal guidance.
CE - Covered Entity

A covered entity is any health plan, health care clearinghouse, and any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA.

BA - Business Associate

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 the CE that involve the use or disclosure of individually identifiable health information.

BAA - Business Associate Agreement

A written agreement between the CE and BA that include certain protections for the information and which imposes specified written safeguards on the individually identifiable health information used or disclosed by its business associates.
Definitions

NOPP - Notice of Privacy Practices
Each covered entity must provide a notice of it’s privacy practices that contain certain elements; It must describe the ways in which the CE may use and disclose protected health information, the CE’s duties to protect privacy, to provide a notice of privacy practices, describe individuals’ rights, include a point of contact for further information and for making complaints to the covered entity.

PHI - Personal Health Information
Any form or media, whether electronic, paper, or oral, 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.

TPO – Treatment, payment and operations
A covered entity may use and disclose protected health information for treatment, payment, and health care operations activities.
Privacy & Security

Privacy having to do with confidentiality of patient information.

Security having to do with the safeguarding of information, systems and data.
HIPAA Refresher

Use and Disclosure of PHI

PHI (Protected Health Information) can be used without a patient authorization for purposes of treatment, payment & healthcare operations or required by law. Other disclosures require a patient’s authorization.

Treatment - Patient care, scheduling, care coordination etc…

Payment - Coding, billing, collections etc..

Healthcare Operations - Utilization review, quality reviews, accreditation, education
Accounting of Disclosures

Prior to HITECH, when information was released without a patient’s authorization outside the treatment, payment or operations (TPO) purposes, the disclosure was required to be accounted for in order to comply with an accounting of disclosures request.

Common types of disclosures without a patient’s authorization are; subpoena, required by law (gunshot wound, abuse, communicable disease etc.) registries such as births, deaths, cancers.

With HITECH, you’ll need to have a process in place that now accounts for your disclosures within the TPO purposes as well.
Minimum Necessary

Minimum necessary means:

Limiting uses and disclosures of PHI to the minimum necessary to perform a particular function.

Examples of not using minimum necessary:

1.) A housekeeper is asked by a patient for a snack. The housekeeper relays the information to the nurse. The nurse tells the housekeeper “No, he has to take his psych meds in an hour and can have a snack then”. Too much information.

2.) An insurance company asks for a copy of a patient’s Jan visit. The clerk copies and sends the patient’s entire file. Too much information.

3.) A schedule of today’s patients is copied and posted at each unit when only two of the nine units utilize the schedule. Too much information.
What is a Breach?

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

-Office of the Civil Rights

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
Breach Examples

Employee sees a patient in the waiting area that she knows. Later on that day, she opens the patient’s file to see the reason for the visit. She discloses that information to a family member.

Employee’s coworker calls off sick and states she was in ER the night before with an elaborate story. The employee looks the coworker up on the registration screen to see if she had an ER visit without accessing any health information.

The file clerk in her routine daily work recognizes a name on a file and opens it to read its contents.
A psychiatrist from New Hampshire was fined $1,000 for repeatedly looking at the medical records of an acquaintance without permission.

A jury in Waukesha, Wisconsin, found that an EMT invaded the privacy of an overdose patient when she told the patient’s co-worker about the overdose out of concern. The jury found that regardless of her intentions, the EMT had no right to disclose confidential and sensitive medical information, and directed the EMT and her employer to pay $3,000 for the invasion of privacy.
Staff Nurse Faces Jail Time for HIPAA Violations

An LPN at an office wrote down information contained in a patient’s record. This patient was known to the LPN in that he was suing her husband from an auto accident. She released the information to her husband whose intent was to use this against the patient. The patient reported the breach to clinic and then the district attorney. The LPN was fired from the practice. The district attorney forwarded the patient's complaint to a federal prosecutor, and within a month, both the LPN and her husband were indicted. LPN was charged with violating HIPAA and with “conspiracy to wrongfully disclose individual health information for personal gain with maliciously harmful intent in a personal dispute”.

She faces up to 10 years in prison, a fine of as much as $250,000, and up to three years of supervised probation. The state nursing board is seeking to revoke her license.
Arkansas Case:
October, 2008, a local television personality was brutally beaten by a home intruder. A physician’s curiosity got the best of him and he logged on to the hospital’s EMR from home. An account rep accessed the patient’s chart 12 times and an ER unit clerk accessed it 4 times.

The doctor received a 2 week suspension from the hospital. In court, the doctor was fined $5,000 and ordered to perform 50 hours of community service by speaking to medical workers about the importance of patient privacy.

The emergency room unit clerk was fired. In court, she was fined $1,500. The account rep was fired and in court received a $2,500 fine.

And many more…. Just Google HIPAA Violations…. 
HITECH ACT

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.

In a Nutshell

HITECH Act:
- Enforcement of the HIPAA regulations with civil penalties $$ $$
- Business Associate requirement to comply with HIPAA regulations
- Breach Notification Requirements
- Requirement to provide an electronic copy of PHI if you have an electronic record
- Patient’s right to request a restriction of disclosure to a health plan
- Marketing & Fundraising restrictions
Enforcement of HIPAA Regulations

The act provides a tiered system for assessing the level of each violation and it’s associated penalty:

**Tier A** - Violations which the offender didn’t realize he/she violated the act and would have handled the matter differently. Fine is $100 for each violation not to exceed $25,000 in a calendar year.

**Tier B** - Violation due to reasonable cause but not willful neglect. Fine is $1,000 for each violation not to exceed $100,000 in a calendar year.

**Tier C** - Violation due to willful neglect that the organization ultimately corrected. Fine is $10,000 for each violation not to exceed $250,000 in a calendar year.

**Tier D** - Violations of willful neglect that the organization did not correct. Fine is $50,000 for each violation not to exceed $1,500,000 in a calendar year.
Tier Examples

Tier A - The employee was not educated on privacy/security measures and would not have known any different.

Tier B - Information released in good faith but later finds out it was a forged signature.

Tier C - Employee willfully breaches a patient’s privacy and the facility/office follows their procedures for corrective action.

Tier D - Employee willfully breaches a patient’s privacy but the facility/office does nothing for corrective action.
What is a Business Associate?

HIPAA defines a business associate as an individual or corporate "person" that performs on behalf of the covered entity any function or activity involving the use or disclosure of protected health information (PHI); and is *not* a member of the covered entity's workforce.

I.e. Copy service, outside transcription company, billing company

**HITECH Act:**

- Require business associates to comply directly with Security Rule provisions
- Comply with HIPAA’s business associate safeguards, including limiting use and disclosure of PHI
Breach Notification Requirements

When a breach has occurred which poses significant harm

You Must:

- Notify the affected patient/individual within 60 days of the discovery of the breach.
- Notify HHS without delay
- Notify the media in breaches that involved 500+ individual’s. Normally done in the form of a press release in the area (TV, paper, website, radio) of the incident within 60 days of discovery and also HHS without delay.
Risk Assessment for Harm

Creating a risk assessment tool is critical in consistently assessing the harm to patients when breaches occur.

A checklist is very helpful in assessing the requirements of breach notification to the patient(s) and HHS.
Assessing a patient’s harm can be difficult. Having a good assessment tool along with policies and procedures will be very important in dealing with breach resolution and notification requirements.

**Things to think about**
- Is the information of a sensitive nature
- Who was the information accessed by or disclosed to
- Would the recipient of the information have reasonably been able to retain the information
- Are there other extenuating circumstances where it would be in the best interest to the patient to notify them
With the HITECH Act, patients have the right to request an electronic copy (i.e. CD, DVD, email) of their record if you have an electronic health record.

HITECH also limits the cost of obtaining copies in electronic format to the labor cost incurred in responding to the request.

Check with your vendor for capabilities of your system to produce an electronic copy.
Patient’s Request for Disclosure Restriction

If an individual desires to pay in full for a procedure or test(s) rather than filing a claim with their insurance, they have the right to restrict disclosure of those services.

Providers should include this restriction (permanently) in their release of information and billing policies and procedures.
Fundraising and Marketing Restrictions

Fundraising communications must clearly provide an opportunity for the recipient of the communication to opt out of receiving future communications. HITECH also provides that if an individual elects to opt out of fundraising communications, the covered entity must treat such election as a revocation of authorization.

Marketing is a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Restrictions apply with HITECH and can be found at the below OCR link.

Example: A hospital releasing the names of patients diagnosed with diabetes this year to a glucose monitoring company for the marketing and sales of their glucose testing machines.

Covered entities should review their HIPAA policies and procedures regarding fundraising and marketing, as well as their notice of privacy practices, to ensure that they are consistent with these requirements.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/marketing.html
HIPAA Refresher

KEY TOOLS

- Office HIPAA policies and procedures
- Audit tool to routinely check for compliance
- Tracking mechanism for accounting of disclosures
- HIPAA related forms
- Notification checklist