Privacy, Confidentiality, and Security

Component 2/Unit 8d

HIPAA privacy and security

- General history of law, identifier standards, and transaction standards already described
- Privacy Rule – went into effect on April 14, 2003
- Security Rule – went into effect on April 21, 2005
- Both revised (aka, HIPAA 2) with ARRA/HITECH legislation in 2009 (Federal Register, 2009; http://www.hhs.gov/ocr/privacy/)
  - Many summaries available (ID Experts, 2009; HIMSS Analytics, 2009; BridgeFront, 2009; Leyva, 2009)

HIPAA Privacy Rule

- Applies to
  - Health care providers
    - Clinicians, hospitals, clinics, etc.
  - Health plans
    - HMOs, insurance companies, etc.
  - Health care clearinghouses
    - Billing services
- Does not apply to treatment, payment, or operations (TPO), i.e., does not preclude health care providers from sharing data for patient care, a not-uncommon misunderstanding (Houser, 2007)

Physician oaths of privacy are not new

- http://www.aapsonline.org/ethics/oaths.htm
- Oath of Hippocrates, 5th century BC
  - "All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and never reveal."
- Declaration of Geneva, 20th century
  - "I will respect the secrets which are confided in me, even after the patient has died."

What is covered?

- Protected Health Information (PHI)
  - Collected from patient and created by covered entity
  - Individually identifiable
  - Electronically transmitted – in reality, all information
- Extends to covered entities or business associates
- De-identified information is not covered
- Pre-emption
  - Federal law is a floor
  - HIPAA takes precedence if state law is contrary
  - State law takes precedence if it is more stringent

Protected health information (PHI)

- Name
- Address (street address, city, county, zip code)
- Names of relatives
- Names of employers
- E-mail address
- Fax number
- Telephone number
- Birth date
- Finger or voice prints
- Photographic images
- Social security number
- Internet protocol (IP) address
- Any vehicle or device serial number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Web URL
- Any other unique identifying number, characteristic, or code

Key privacy compliance areas

- Notice of privacy practices
- Authorization
- Business associates
- Allowable disclosures
- Marketing
- Physician and staff training
- Penalties

Notice of privacy practices (NPP)

- Patient has right to
  - Adequate notice of privacy practices
  - Uses and disclosures of PHI
  - Description of individual rights
  - Covered entities' legal duties
- One problem is readability of NPP forms comparable to medical journal articles and beyond 80% of US adults (Breese, 2005)
- Physicians' requirements for obtaining NPP consent include
  - "Good faith effort" to obtain acknowledgement during first provision of in-person service
  - Failure to obtain is not penalized (per Bush administration revision)

Other aspects of privacy practices

- Must be written in plain language
- Practices/organizations must state they preserve the right to change notice of privacy practices
- There must be a complaint process
- Practices/organizations must designate a privacy official in the office
- See OHSU examples of Notice of Privacy Practices (NPP)
  - http://www.ohsu.edu/xd/about/services/integrity/ips/npp.cfm/

Authorizations

- Providers must obtain an authorization before using PHI for purposes other than TPO
- They may not condition treatment on an individual's authorization
- Covered entities must make "reasonable safeguards" to limit the use or disclosure of PHI to the minimum amount necessary
  - Non-TPO disclosure governed by "Minimum Necessary" standard (HHS OCR, 2003)

Authorizations must include

- Names of authorized persons making use or disclosure
- Description of information
- Expiration of date of event
- Patient's right to revoke and instructions on how to do so
- Purpose of use or disclosure
- Signature and date

Business associates (BAs)

- Agents, contractors, or others hired to do work of or for covered entities (CEs) that requires PHI, such as
  - Billing companies
  - Vendors (with access to PHI)
- In original HIPAA, had to obtain "satisfactory assurances" of privacy protections, but in HITECH, BAs now required to meet same rules for covered entities
  - Each BA must sign agreement with CE
  - BAs subject to breach notification rules
  - BAs include health information exchanges, PHR vendors, etc.

Allowable non-TPO disclosures

- Research
  - Overview: HHS, 2004
  - Authorization by patient is generally required
  - Authorization waiver can be provided by an Institutional Review Board (IRB) or Privacy Board approval
    - Must involve "no more than a minimal risk"
    - Research could not be practically conducted without waiver and without access to PHI
- Public Health
  - Can be disclosed to public health agencies for public health activities
  - Also allowed for child abuse reporting, exposure to communicable diseases, and workforce surveillance
- Other
  - Law enforcement
  - Decedents
  - Cadaveric tissue donation

Marketing

- Defined as "a communication about a product/service that encourages recipients of the communication to purchase/use the product/service"
- Is not marketing for providers if treatment is
  - Therapy recommendation
  - Appointment notification
  - Prescription refills

Physician and staff training

- Practices/organizations must
  - Designate a Privacy Officer
  - Develop policies and procedures
  - Provide privacy training to workforce
  - Develop a system of sanctions for employees who violate the privacy law
- Con$ultant$ are standing by to help!

Penalties

- Original HIPAA criticized for modest penalties and minimal prosecutions
- HITECH increases severity of penalties
  - Tiered penalty structure ranging from $25,000 to $1.5M
  - Application of "willful neglect"
  - Allows state attorney generals to sue in federal courts
  - Enforced by HHS Office of Civil Rights (OCR, http://www.hhs.gov/ocr/privacy/)

Does HIPAA Privacy Rule protect privacy?

- Reviews by NCVHS (Lumpkin, 2004) and GAO (2004) found adherence less problematic than anticipated
- Major concerns relate to difficulty in performing clinical research
  - Finding and accessing patients for research more difficult (Armstrong, 2005)
  - Two-thirds of researchers surveyed reported more difficulty in work while only one-quarter believed privacy enhanced (Ness, 2007)
  - Reports from AAHC (2008) and IOM (2009) argue for revision to make research easier
- Also concerns with implications for public health (Kamoie, 2004)
- Another view calls for less emphasis on consent and more on a framework that makes for easier sharing of TPO (with some modifications of "O") with more rigorous restrictions on other uses, such as marketing (McGraw, 2009; McGraw, 2009)

Other modifications in HITECH

- Breach notification – when over 500 patients, must be reported to local media and HHS OCR
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html
- Restrictions on disclosures
  - Services paid for out of pocket can be withheld from record
  - TPO disclosures must be tracked and records maintained for three years
  - CEs with EHRs must provide or transmit PHI in electronic format as directed by patient
- Patients can opt out of fundraising appeals