Privacy, Confidentiality, and Security

Component 2/Unit 8b

Privacy, confidentiality, and security

- Definitions
- Concerns
  - Privacy
  - Security
- Tools for protecting health information
- HIPAA
  - Privacy Rule
  - Security Rule
  - Additions in HITECH
  - Implications

Definitions

- Privacy – right to keep things to yourself
- Confidentiality – right to keep things about you from being disclosed to others
- Security – protection of your personal information
- Individually identifiable health information (IIHI) – any data that can be correlated with an individual
- Personal health information – IIHI as defined by HIPAA Privacy Rule
- Consent – (in context of privacy) written or verbal permission to allow use of your IIHI

Concerns about privacy

- Personal privacy vs. common good
- Continued disclosures
- Concerns of public
- De-identified data

Personal privacy vs. the common good

- There is a spectrum of views
  - One end holds that while personal privacy is important, there are some instances when the common good of society outweighs it, such as in biosurveillance (Gostin, 2002; Hodge, 1999)
  - The other end holds that personal privacy trumps all other concerns (Privacy Rights Clearinghouse, 2009; see also Deborah Peel, MD and www.patientprivacyrights.org)
    - Concerns expressed in ACLU video (ACLU, 2004)
  - More balanced views? – CHCF, 2008; ACP, 2009
- Where do your views fit?

There continue to be patient information disclosures

- Google can pick up not only patient data, but also access points to databases, which may not be well protected (Chin, 2003)
- Portland, OR – Thieves broke into a car with back-up disks and tapes containing records of 365,000 patients (Rojas-Burke, 2006)
- Several episodes from VA, e.g., laptop with data of >1 million veterans, recovered without apparent access (Lee, 2006)
- HIMSS Analytics report (2008) found aggregated data in hospitals and healthcare facilities richest source for fraud and abuse; over 1.5 million names exposed in 2006-2007
- HITECH now requires notification of breaches of over 500 individuals under HIPAA
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

Healthcare organizations are not well-prepared for security

- Deloitte, 2009
  - Data leakage is a primary threat
  - Identity and access management is a top priority
  - Trend towards outsourcing raises many third-party security concerns
  - Role of Chief Information Security Officer (CISO) has taken on greater significance
  - As security environment becomes more complex and regulation continues to grow, security budgets not keeping pace
- HIMSS, 2009
  - Healthcare organizations not keeping pace with security threats and readiness for them

Technology can worsen the problem

- USB ("thumb") drives run programs when plugged into USB port; can be modified to extract data from computer (Wright, 2007)
- Personal health records based on Microsoft Access can easily have encryption compromised (Wright, 2007)
- 10% of hard drives sold by a second-hand retailer in Canada had remnants of personal health information (El Emam, 2007)

What is the role of governments?

- In US, GAO has criticized government inaction for protecting data in its systems and developing policy (Koontz, 2007)
- NCVHS recommendations
  - 26 recommendations for policy concerning health privacy for the Nationwide Health Information Network (NHIN) (Cohn, 2006)
  - Further elaborated recommendations for personal control and call for consistent and coherent policy (Cohn, 2008)
- Health Information Security and Privacy Collaboration (HISPC) has assessed 42 states and territories, finding diverse approaches and laws, making nationwide approaches difficult (HHS, 2010)

Role of governments (cont.)

- Nationwide Privacy and Security Framework (2008) based on principles
  - Individual access
  - Correction
  - Openness and transparency
  - Individual choice
  - Collection, use, and disclosure limitation
  - Data quality and integrity
  - Safeguards
  - Accountability
- Not surprisingly, some believed did not go far enough (Conn, 2008)
- Further work has laid out approach to identifying stakeholders and eliciting consumer preferences for access and exchange of personal health data (HHS, 2009)

What do other governments do?

- European Commission Directive 95/46/EC (EC, 2007)
  - Stringent rules allow data processing only with consent or highly specific circumstances (legal obligation, public necessity)
  - Countries that implement Directive 95/46/EC provide examples for how "consent" for use of information on Nationwide Health Information Network (NHIN) may proceed in US (Pritts, 2007)

Related issues for medical privacy

- Who "owns" medical information?
  - Easier to answer with paper systems, but growing view is the patients own it, which has economic implications (Hall, 2009; Rodwin, 2009)
- "Compelled" disclosures (Rothstein, 2006)
  - We are often compelled to disclose information for non-clinical care reasons
- The ultimate "personal identifier" may be one's genome (McGuire, 2006)
  - Even "de-identified" data may compromise privacy (Malin, 2005)
  - Genome of family members can identify siblings (Cassa, 2008)
  - Data from genome-wide association studies can reveal individual level information (Lumley, 2010)

The public is concerned

- Harris Interactive, 2005
  - Split between saying benefits outweigh risks of EHRs (48%) vs. risks outweigh benefits (47%)
  - 70% somewhat or very concerned that sensitive health information might be leaked due to inappropriate security
  - 82% desire tools to track their own information and assert privacy rights from start
- CHCF, 2005
  - 67% somewhat or very concerned about privacy of their medical records
  - 52% somewhat or very concerned that their employers might misuse their medical information
  - Consumers generally unfamiliar with HIPAA

AHIMA Health Information Bill of Rights (AHIMA, 2009)

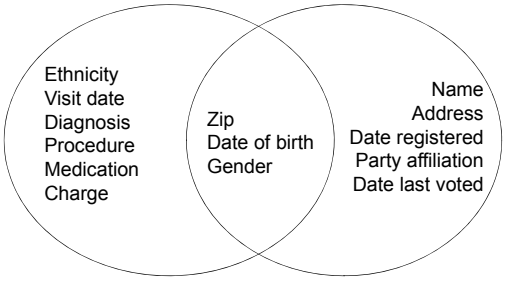
- The right to access your health information free of charge
- The right to access your health information during the course of treatment
- The right to expect that your health information is accurate and as complete as possible
- The right for you or your personal representative(s) to know who provides, accesses, and updates your health information, except as precluded by law or regulation
- The right to expect healthcare professionals and others with lawful access to your health information to be held accountable for violations of all privacy and security laws, policies, and procedures, including the sharing of user IDs and passwords
- The right to expect equivalent health information privacy and security protections to be available to all healthcare consumers regardless of state or geographic boundaries or the location (jurisdiction) of where the treatment occurs
- The right to the opportunity for private legal recourse in the event of a breach of one's health information that causes harm

- See also: HealthDataRights.org

So maybe "de-identified" data is more secure? Not necessarily

- Sweeney, 1997; Sweeney, 2002
  - 87% of US population uniquely identified by five-digit zip code, gender, and date of birth
  - Identified William Weld, governor of Massachusetts, in health insurance database for state employees by purchasing voter registration for Cambridge, MA for $20 and linking zip code, gender, and date of birth to "de-identified" medical database
- Genomic data can aid re-identification in clinical research studies (Malin, 2005; Lumley, 2010)
- Social security numbers can be predicted from public data (Acquisti, 2009)

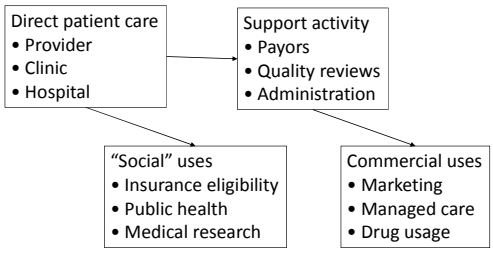
How Governor Weld was de-identified



Concerns about security

- Many points of leakage
- A problem for paper too
- Consequences of poor security
- Medical identity theft

Flow of information in healthcare – many points to "leak"



(Rindfleisch, 1997)

Security for paper records is a significant problem as well

- Difficult to audit trail of paper chart
- Fax machines are easily accessible
- Records frequently copied for many reasons
  - New providers, insurance purposes
- Records abstracted for variety of purposes
  - Research
  - Quality assurance
  - Insurance fraud → Health Information Bureau (Rothfeder, 1992)

Potential consequences of poor security

- Rindfleish, 1997
  - Patients avoid healthcare
  - Patients lie
  - Providers avoid entering sensitive data
  - Providers devise work-arounds
- CHCF, 2005
  - 13% of consumers admit to engaging in "privacy-protective" behaviors that might put health at risk, such as
    - Asking doctor to lie about diagnosis
    - Paying for a test because they did not want to submit a claim
    - Avoid seeing their regular doctor

Medical identity theft

- A growing concern, emanating from general identity theft, defined as use of IIHI for obtaining access to property or services (AHIMA, 2008)
  - Victims are not only individuals but also health providers and plans as well as society at large
  - Value of medical identity information much higher than just Social Security number
- HHS report outlines approaches to prevention, detection, and remediation (2009)