Privacy, Confidentiality, and Security: Basic Concepts

WILLIAM HERSH, MD
OREGON HEALTH & SCIENCE UNIVERSITY

Privacy, confidentiality, and security

- Definitions
- Concerns
  - Privacy
  - Security
- Tools for protecting health information
- Approaches to protecting health information

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)
- 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?

- United States: HIPAA (Leyva, 2010)
  - Privacy Rule defines policies, including “treatment, payment, and operations” (TPO)
  - Security Rule specifies required protections
- European Commission Directive 95/46/EC (EC, 2007)
  - Stringent rules allow data processing only with consent or highly specific circumstances (legal obligation, public necessity)

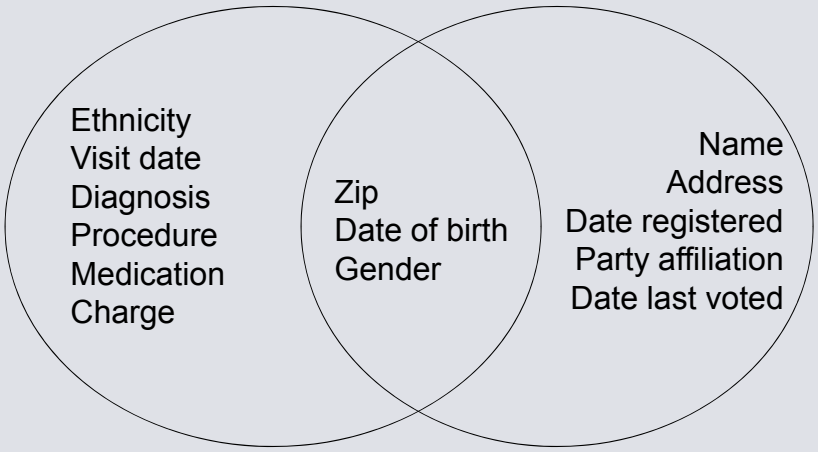
Related issues for medical privacy

- 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)

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)

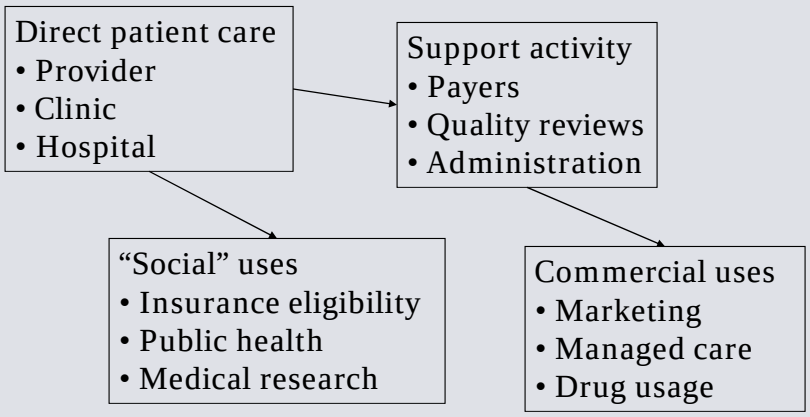
How Governor Weld was de-identified



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

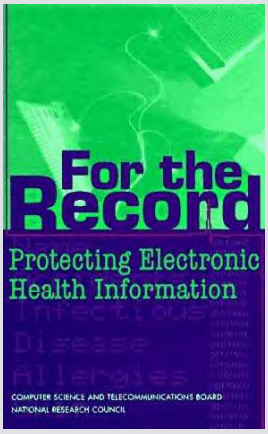
- Difficult to audit trail of paper chart
- Fax machines are easily accessible
- Records frequently copied for many reasons
  - New providers, insurance purposes
- Records abstracted for variety of purposes
  - Research
  - Quality assurance
  - Insurance fraud → Health Information Bureau (Rothfeder,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

Tools for protecting health information

- IOM report: *For the Record* (1997)
- Report commissioned by NLM; informed HIPAA legistation
- Looked at current practices at six institutions
- Recommended immediate and future best practices
- Some content dated, but framework not



Threats to security

- Insider
  - Accidental disclosure
  - Curiosity
  - Subornation
- Secondary use settings
- Outside institution
  - A lot of press, few examples

Technologies to secure information

- Deterrents
  - Alerts
  - Audit trails
- System management precautions
  - Software management
  - Analysis of vulnerability
- Obstacles
  - Authentication
  - Authorization
  - Integrity management
  - Digital signatures
  - Encryption
  - Firewalls
  - Rights management

HiBBs

Encryption

- Necessary but not sufficient to ensure security
- Should, however, be used for all communications over public networks, e.g., the Internet
- Information is scrambled and unscrambled using a key
- Types: symmetric vs. asymmetric
  - Asymmetric, aka public key encryption, can be used for digital certificates, electronic signatures, etc.

HiBBs

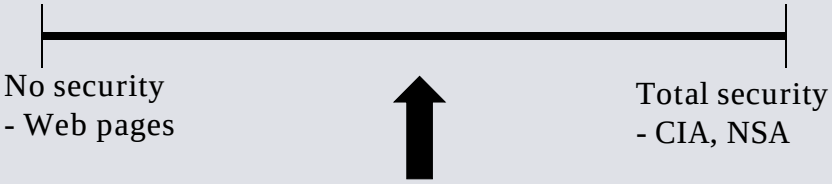
NRC report best practices

- Organizational
  - Confidentiality and security policies and committees
  - Education and training programs
  - Sanctions
  - Patient access to audit trails
- Technical
  - Authentication of users
  - Audit trails
  - Physical security and disaster recovery
  - Protection of remote access points and external communications
  - Software discipline
  - Ongoing system vulnerability assessment

Authentication and passwords

- Authentication is process of gaining access to secure computer
- Usual approach is passwords (“what you know”), but secure systems may add physical entities (“what you have”), e.g.,
  - Biometric devices – physical characteristic, e.g., thumbprint
  - Physical devices – smart card or some other physical “key”
- Ideal password is one you can remember but no one else can guess
- Typical Internet user interacts with many sites for which he/she must use password
  - Many clamor for “single sign-on,” especially in healthcare, where users authenticate just once (Pabrai, 2008)

Health information security is probably a trade-off



Where is the happy medium for healthcare?

Other issues about privacy and confidentiality to ponder…

- Who owns health information?
- How is informed consent implemented?
- When does public good exceed personal privacy?
  - e.g., public health, research, law enforcement
- What conflicts are there with business interests?
- How do we let individuals "opt out" of health information systems?
  - What are the costs? When do we override?