Practical Approaches to Privacy

Deven McGraw

CENTER FOR DEMOCRACY & TECHNOLOGY

The Health Privacy Project at CDT

- Health IT and electronic health information exchange are the engines of health reform & have tremendous potential to improve health care quality, reduce costs, and empower consumers.
- Some progress has been made on resolving the privacy and security issues raised by e-health – but questions remain and implementation challenges loom.
- Project's aim: Develop and promote workable (or "practical") privacy and security policy solutions for personal health information.

People want Health IT - but also have significant privacy concerns

- Survey data shows the public wants electronic access to their personal health information.
- But a majority - 67% - also have significant concerns about the privacy of their medical records (California Healthcare Foundation 2005).

Consequences of Failing to Act

- Protecting privacy is important
  - Prevents harm
  - Good health care depends on accurate and reliable information
- Without privacy protections, people will engage in “privacy-protective behaviors” to avoid having their information used inappropriately.
  - 1 in 6 adults withhold information from providers due to privacy concerns. (Harris Interactive 2007)
  - Persons in poor health, and racial and ethnic minorities, report even higher levels of concern and are more likely to engage in privacy-protective behaviors. (CHF 2005)

Impact on Individual and Public Health

- Quality of individual care may suffer;
- A provider's ability to diagnose and treat accurately may be impaired;
- Cost of care escalates as conditions are treated at a more advanced stage or are spread to others; and
- Research, public health, and quality initiatives may be undermined due to incomplete or inaccurate data.

Health IT Can Protect Privacy - But Also Magnifies Risk

- Technology can enhance protections for health data (for example, encryption; role-based access; identity proofing authentication)
- But moving health information into electronic form - in the absence of strong privacy and security safeguards - magnifies the risks.
  - Recent thefts of laptops, inadvertent posting of data on the Internet
  - Cumulative effect of these reports deepens consumer distrust

A Comprehensive Approach is Needed

- Privacy and security protections are not the obstacle - enhanced privacy and security can be an **enabler** to health IT.
- A comprehensive privacy and security framework is needed to facilitate health IT and health information exchange.
  - Fair information practices
  - Sound network design
  - Accountability/Oversight

Common Framework Includes Network Design Characteristics

- Also key to protecting privacy and security
- Recommend a “network of networks” distributed architecture
- Key elements also include interoperability and flexibility, which support innovation and create opportunities for new entrants

Role of HIPAA in New Environment

- HIPAA Privacy and Security Rules reflect elements of this framework and provide important protections governing access, use and disclosure of PHI by health system entities.
- But the existing regulations are insufficient to cover the new and rapidly evolving e-health environment.
- Effective enforcement also has been lacking.
- State laws often provide stronger protections – but gaps remain

“Next Generation” of Health Privacy

- Build on HIPAA for traditional health care entities – address “who is covered” and “what protections are in place”
- Establish new protections to address concerns raised by access to information outside of the health care system
- Hold all holders of health data accountable for complying with baseline protections

Provisions of HITECH/ARRA

- Filled a number of gaps in HIPAA
  - “Business associates” now directly accountable for complying with most (but not all) HIPAA privacy and security regs (and HIEs/RHIOs are considered to be BAs)
  - Breach notification provisions go into effect on September 24, 2009; exception for data that is encrypted
  - Strengthened right for patients to receive an accounting of disclosures from their record
  - Patients who pay out of pocket can request that data not be sent to their health plan
  - Strengthened rules re: use of data for marketing
  - Patient right to receive electronic copy from electronic health/medical record

Filling gaps in HIPAA (cont.)

- Stronger enforcement
  - State AGs now authorized to enforce
  - Civil monetary penalties increased
  - HHS required to impose penalties in cases of willful neglect
  - HHS required to do privacy and security audits

Still Work to be Done

- Personal Health Records
  - Currently not covered by HIPAA if offered by Microsoft, Google, Dossia, WebMD & others (except if HIPAA business associate provisions apply)
  - ARRA established breach notification requirements, strengthened right to receive electronic copy of data
  - HHS (working with FTC) to provide recommendations to Congress by 2/2010 on privacy & security protections

Work to be Done (cont.) - PHRs

- Need consistent regulation – but HIPAA as currently structured is not the answer
  - Treatment, payment & operations exception makes little sense for PHRs, which should be consumer controlled
  - Reliance on authorization for marketing & business uses provides weak protection
  - Markle Common Framework for Networked Personal Health Information provides good model
  - FTC should play a role in regulating PHRs

Work to be Done (cont.)

- Implementation of new rules will take ***a lot*** of work
  - Education about new rights, responsibilities
  - Hope is that HHS will take a more active role in privacy “stewardship”
- Uses of data for marketing purposes – implementation of new provisions key
- Strengthening de-identification standard and establishing clear rules against, and penalties for, re-identification

Work to be Done (cont.)

- Enacting limits on use of health information to discriminate in employment and insurance
- Clear policies regarding access to information in electronic health information networks/exchanges
- Data protections for additional uses created by created by health reform (e.g., insurance “connectors”)

Appropriate Role of Patient Consent

- Public debates about privacy protection have focused disproportionately on whether patients should be asked to authorize all uses of their information.
- Individual control is an important component of fair information practices - but it is just one component.

Patient Consent (cont.)

- Providing greater authorization rights is not the sine qua non of privacy
  - Places most of the burden of privacy protection on the individual at a time when they are least able to make complicated decisions about the use of their data.
  - Research shows that patients do not read consent forms - and if they do read them, they frequently do not understand them and inherently believe they protect privacy even in cases where the opposite is true.

Consent (cont.)

- The adoption of a comprehensive privacy and security framework that governs the access, use and disclosure of health information will better protect privacy in e-health systems.
- But health systems should be engineered to honor (and appropriately manage) patient consent where such consent is legally required or voluntarily sought.
- In addition, patients should be given some right to at least opt out of having their information accessible through networks, particularly network policies allow for broad information sharing for a range of purposes

For privacy to enable health IT, we need to "enable" privacy

deven@cdt.org