KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

CENTER FOR DEMOCRACY
& TECHNOLOGY

Emerging Issues in Health Privacy:

Perspective of a Privacy Advocate

Deven McGraw
Director, Health Privacy Project

March 9, 2011

Health Privacy Project at CDT

- Health IT and electronic health information exchange are engines of health reform with tremendous potential to improve health, reduce costs and empower patients.

- Some progress has been made on resolving the privacy and security issues raised by e-health – but gaps remain and implementation challenges loom.

- Project's aim: Develop (papers) and promote (advocacy) workable 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; more recent AHRQ focus groups and 2011 Markle survey confirm).

Consequences of Failing to Act

- 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)

Health IT Can Protect Privacy – But Also Magnifies Risks

- Technology can enhance protections for health data (for ex., encryption; role-based access; identity proofing & authentication; audit trails)
- But moving and storing health information in electronic form – in the absence of strong privacy and security safeguards – magnifies the risks
  - Thefts of laptops, inadvertent posting of data on the Internet, reports of internal "snooping"
  - Increased media attention to data captured 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.
  - The essence of what we mean by “workable” protections
- A comprehensive privacy and security framework is needed to facilitate health IT and health information exchange.
  - Fair information practices – strong data stewardship model; consent plays important role but is not linchpin
  - Sound network design
  - Accountability/Oversight

Fair Information Practices – Markle Common Framework

- Openness and transparency
- Purpose specification and minimization
- Collection limitation
- Use limitation
- Individual participation and control
- Data integrity and quality
- Security safeguards and controls
- Accountability and Oversight
- Remedies

Role for Individual Consent

- Public debates about privacy protection until recently have focused almost exclusively 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.
- Providing greater authorization rights is not the best way to protect privacy and security.

Why Not Just Enhance Consent Rights?

- Places most of the burden of privacy protection on the individual.
- 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.
  - Blanket authorizations in particular can easily become shields for inappropriate uses
- Instead, provide & honor individual’s meaningful choices about non-routine or unexpected uses of data

“Next Generation” of Health Privacy

- Build on HIPAA for traditional health care entities – no need to rip and replace (HITECH took the first step here)
- Establish protections for health information that migrates outside of the HIPAA bubble
- Address concerns raised by new HIT infrastructure (such as HIEs)
- <u>Essentially, hold all entities who handle health data accountable for complying with baseline protections</u>

Emerging Issues/Agenda for the Future

- Successful implementation of new HITECH privacy provisions
- Address issues raised by the use of HIEs or data exchange “intermediaries”
  - Are business associate rules sufficient?
- Protections for health data that is outside the HIPAA bubble
  - Will new consumer privacy efforts (FTC & Commerce reports, HHS Roundtable on PHRs, draft legislation) pay off for health information?
- Framework for secondary data uses – for ex., comparative effectiveness research
  - Distributed data networks

Agenda for the future (cont.)

- Policies for de-identified data – focus on robust methodologies, prohibit re-identification
  - Also – encouraging use of “less identifiable” data for routine purposes; possible interpretation of minimum necessary standard?
- Better enforcement & active policy “stewardship” by regulators
  - Issuance of guidance, clarifications, FAQs
  - Safe Harbors?
  - Regulation of business associates

Questions?

Deven McGraw

202-637-9800 x115

deven@cdt.org

www.cdt.org/healthprivacy

cdt KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE