

Privacy & Security Policy and the New Political Landscape

Deven McGraw

CENTER FOR DEMOCRACY & TECHNOLOGY

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)

Health IT Can Protect Privacy - But Also Magnifies Risk

- HIMSS members know well the privacy and security tools that can be employed in electronic records.
- 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 is 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

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 regulations are insufficient to cover the new and rapidly evolving e-health environment.
- ❑ Effective enforcement is also lacking.

“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
- Ensure patients trust infrastructure so that information sharing for treatment purposes can occur

Core Issues

- ▣ Making sure individuals are protected regardless of where data sits or flows:
 - ▣ RHIOs, HIEs not covered by HIPAA; no requirement to be business associates
 - ▣ Information now being managed by Internet companies, employers (through PHRs, websites)
- ▣ Strengthen enforcement
 - ▣ Entities not directly covered by HIPAA?
 - ▣ Lack of adequate resources

Core Issues (cont.)

- ▣ Greater needs for anonymous data
 - ▣ Viability of de-identification and limited data set standards
 - ▣ Accountability for inappropriate re-identification?
- ▣ Lack of federal breach notification requirement
- ▣ Appropriate role for consent
 - ▣ Places greater burden on individuals
 - ▣ But in absence of regulation...

Core Issues (cont.)

- ▣ Ensure individuals can obtain electronic copies
- ▣ In light of broader health information exchange, consider tightening rules for:
 - ▣ Marketing
 - ▣ Audit trails
 - ▣ Access to information for health care operations

For privacy to enable health IT, we
need to “enable” privacy

deven@cdt.org

CENTER FOR DEMOCRACY & TECHNOLOGY