



Privacy & Security Issues & Personal Health Records (PHRs)

Deven McGraw

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).

EMRs

- ❑ Covered by the HIPAA Privacy and Security Rules
- ❑ HIPAA protections enhanced by provisions in ARRA/HITECH

What about PHRs?

- ❑ Covered by HIPAA if offered by a covered entity or business associate
- ❑ Not covered by HIPAA if offered by an independent vendor
- ❑ In some cases, independent vendors may be business associates of covered entities
 - ❑ Provision in ARRA yet to be interpreted
- ❑ Right to electronic copy – can direct to PHR

If not covered by HIPAA, then what?

□ FTC Act

- Must abide by privacy policies
- Must adopt reasonable security protections

□ Breach notification provisions in ARRA

□ Other federal laws that apply to Internet-based companies, electronic storage media

- None provide comprehensive privacy and security framework

□ State laws

HHS/FTC Study

- ▣ ARRA requires HHS (working with FTC) to report to Congress on privacy & security recommendations for PHR vendors not covered by HIPAA
 - ▣ Due February 18, 2010
- ▣ Study must include recommendation for which agency should regulate vendors

Should HIPAA apply?

- HIPAA permits broad information sharing for treatment, payment & health care operations (as well as disclosures for public health and some research purposes without patient consent).
- Right approach for health system entities – wrong approach for a tool intended to be used by the consumer.
 - Rules for marketing uses also too permissive
- Other parts of HIPAA may be applicable

What protections should be in place?

- ❑ Markle Common Framework for Networked Personal Health Information sets forth consensus policies for PHRs
- ❑ www.connectingforhealth.org/phti
- ❑ Endorsed by wide array of stakeholders, including major PHR vendors & consumer groups, AHIP

Elements of Framework

- ❑ Policies & technical security requirements
- ❑ Based on fair information practices tailored to PHRs
- ❑ Examples:
 - ❑ Consumer consent and control over access to information in the PHR
 - ❑ Mechanisms for resolving disputes (such as errors & data quality)
 - ❑ Access to information
 - ❑ Audit trails

“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

Difficult Issues

- ❑ Making sure individuals are protected regardless of where data sits or flows
- ❑ Separate rules for EMRs & PHRs – sustainable over the long term?
- ❑ Evolving area of consumer health applications

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

deven@cdt.org