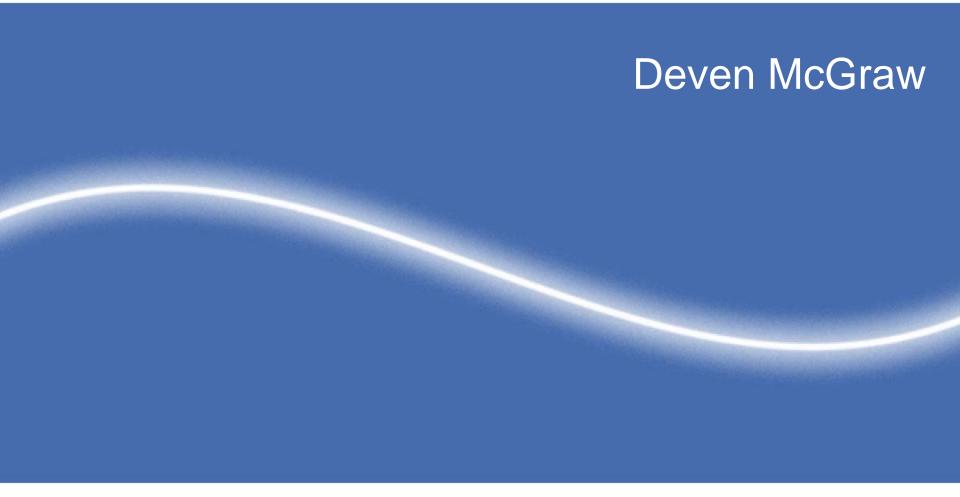
Concerns of a Privacy Advocate – and How to Respond



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 ehealth – but gaps remain and implementation challenges loom.
- Project's aim: Develop and promote 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 confirm).

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 privacyprotective behaviors. (CHF 2005)

Health IT Can Protect Privacy - But Also Magnifies Risk

- Technology can enhance protections for health data (for example, encryption; rolebased access; identity proofing & authentication)
- But moving & storing health information in 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, "snooping"
- CEN Cumulative effect of these reports deepens o Logy 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 strong data stewardship model
 - Sound network design
 - Accountability/Oversight

"Next Generation" of Health Privacy

- Build on HIPAA for traditional health care entities (ARRA took first steps here)
- Establish new protections to address concerns raised by access to information outside of the health care system
- Hold all who handle health data accountable for complying with baseline protections

ARRA (Title XIII- HITECH)

- Broke the privacy "logjam"
- Most significant change to the healthcare privacy and security environment since the original HIPAA privacy rule
- Not a change to everything about HIPAA but some significant changes that will need to be addressed by many entities handling health care information
- Most provisions require further regulatory clarification

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 23, 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
 - Prohibition on sales of protected health information
 - Strengthened rules re: use of data for marketing
 - Patient right to receive electronic copy from electronic health/medical record OCRACY & TECHNOLOGY

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.)

- Successful implementation of new rules
- Addressing downstream or "secondary" uses of data by trading partners
- □ Tight implementation of new marketing provisions
- Addressing "identifiability" of data through minimum necessary guidance and better de-identification policy plus strict penalties for re-identification
- Sound policies to govern (and build trust in) exchange through networks

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

deven@cdt.org