HIPAA Privacy:
Perspective of a Privacy Advocate

Deven McGraw
Director, Health Privacy Project
February 20, 2013

Health Privacy Project at CDT

- Our theory: Privacy = *enabler* to flows of data that have the potential to improve individual, public and population health
- Aim is to build public trust in these data flows.
- Without privacy protections, people will engage in "privacy-protective behaviors" to avoid having their information used inappropriately.

People want Health IT - but also have significant privacy concerns

- Survey data shows the public supports electronic health information exchange among providers and patients.
- But a majority also have significant concerns about the privacy of their medical records (consistent survey results over the past 7 years).
- 1 out of 6 surveyed practice “privacy-protective behaviors” due to concerns about privacy
- Privacy should “enable” health information exchange by bolstering public trust

Health IT Can Protect Privacy – Also Magnifies Risk

- Technology can enhance protections for health data (encryption; role-based 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”
  - 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 e-health.
- A comprehensive privacy and security framework is needed
  - Fair information practices – strong data stewardship model; consent plays important role but is not linchpin
  - Sound network design – for ex., distributed networks vs. centralized databases
  - Accountability/Oversight
- Markle Common Framework provides good implementation example

HIPAA Omnibus Rule (issued January 2013)

- Biggest win for consumers and patients = issuance of the final rule!
- Provisions include a number of important advances for consumers, including:
  - Breach notification standard
  - Marketing & Fundraising
  - Accountability of data chain (BAs & subcontractors)
  - Individual access to data (glass half full)
  - Immunization and Decedent's records

What's not in the Omnibus Rule

- Right of individuals to get an accounting of access to or disclosures of their health information (aka "Accounting of Disclosures") – still in process
- Methodology for giving individuals "harmed" by HIPAA violations a percentage of any civil monetary penalties or settlements collected (HITECH Section 13409(c)(3)) – no rule proposed yet
- No release yet - report on privacy protections for PHRs not covered by HIPAA and guidance on implementation of minimum necessary standard
- HITECH also mandated study of definition of "psychotherapy notes" – no specific deadline for the study

HIPAA Omnibus Rule (issued January 2013)

- Breach notification standard
  - Presumption that notification is required unless low probability that information was compromised
  - Risk assessment based on 4 factors (what happened to the data)
  - Problem with harm standard was it invited subjective judgments about value of breached data to an individual

HIPAA Omnibus Rule (issued January 2013)

- Marketing Rule
  - If communication is paid for by manufacturer of the product or service being pitched, it is marketing and requires prior authorization (no confusing distinction between treatment and population communications)
  - Public policy exception for communications about drugs (incl. generics) patient is already taking (as long as remuneration for the communication is reasonable).
  - Face to face communications still exempt.

HIPAA Omnibus Rule (issued January 2013)

- Fundraising (for the covered entity)
  - More data can be used for fundraising purposes BUT
  - Right to opt-out is strengthened

HIPAA Omnibus Rule (issued January 2013)

- Accountability of Data Chain
  - BA to subcontractor to subcontractor….
  - BAA is required – but whether it exists or not does not settle the question of whether or not a contractor has BA status under the law
  - Must have capability to routinely access PHI (includes data storage services but not “mere conduits)
  - Must be performing certain services “on behalf of” a covered entity – commercial PHRs not covered, for example.

HIPAA Omnibus Rule (issued January 2013)

- Individual access to data
  - More than in an EHR – data kept electronically in a designated record set.
  - Patients can't dictate form if CE/BA can't produce – but CE/BA must have capability to produce some electronic copy in machine readable form
  - Patients can get data sent by unsecure e-mail!
  - Patients seeking to have data transmitted directly to a third party must submit request in writing, signed, with with address of recipient
  - BUT can still take up to 30 days to produce; additional 30 days if off-site

HIPAA Omnibus Rule (issued January 2013)

- Immunizations & decedents
  - Can disclose immunization records to schools with consent (not required to meet strict HIPAA authorization requirements)
  - Can decedent's info to family members & others involved in the person's care (even immediately after death) unless entity was aware that such disclosure would be inconsistent with the patient's prior expressed preferences.

Questions?

Deven McGraw

202-637-9800 x115

deven@cdt.org

www.cdt.org/healthprivacy

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE