KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

HIPAA Privacy:
Perspective of a Privacy Advocate

Deven McGraw
Director, Health Privacy Project
February 6, 2014

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.

Omnibus is in effect

- 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)
- Provisions also eased HIPAA research provisions

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

- 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

- 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).
    - ➢ Recent guidance helpful
  - Face to face communications still exempt.

HIPAA Omnibus Rule

- 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

- 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

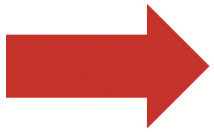
- Research authorizations
  - Previously required to be very specific.
  - No change in actual regulatory language; however, preamble puts forward a more flexible approach.
  - Authorizations are worded in a way that an individual would reasonably expect that his/her PHI would be used for that particular research. Applies to:
    - Description of information to be used in research, and
    - Description of the type of research (purpose).

What's next?

- OCR enforcement
  - BA audits
  - Emphasis on security risk analysis
  - Emphasis on patient access to health information
  - Impact of change in leadership?
- Release of final rule on direct patient access to lab data
- Will meaningful use Stage 2 – which provides patients with direct access to downloadable data – shine a spotlight on lack of protections for health data outside of HIPAA?
- Accounting for Disclosures?

Health IT Policy Committee & AOD

- Held virtual hearing on 9/30/13; collected public comments via Health IT Buzz Blog; issued recommendations to HHS on 12/4/13.
- Focus implementation on disclosures *outside* of a provider or OHCA "electronic health record" (HITECH mandate)
- Pilot technologies and policy approach prior to moving forward with regulatory changes
- Report to patients (upon request) should list name of entity receiving data, not individual name (similar to Fair Credit Reporting Act)



Questions?

Deven McGraw

202-637-9800 x115

deven@cdt.org

www.cdt.org/healthprivacy

cdt KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE