Privacy of Digital Health Data:

Are we there yet?

Deven McGraw, JD, MPH, LLM
Director, Health Privacy Project

July 25, 2013

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" with the providers and payers due to concerns about privacy
- Privacy should "enable" health information exchange by bolstering public trust

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

At the same time….

- 80% of Internet users look for health information on-line
- Nearly 500 health social networking sites (est.) – nearly 500 (up from 35 four years ago) (Health 2.0)
- 7% of patients use PHRs – but that number has doubled since 2008 (California Healthcare Foundation); could increase after 2014 due to view/download & transmit provisions in Stage 2
- 500M people will be using mobile health apps by 2015 (research2guidance)
- Most consumer-facing health tools not covered by health privacy laws

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Ongoing Privacy Challenges

- Education about rights and responsibilities (both for patients and health data holders)
  - Critical to implementation of new HITECH provisions
  - Busting persistent myths about HIPAA
- Taking data security seriously
- Protections for health data shared outside of HIPAA coverage bubble
- Facilitating a "learning health care system" through data re-use

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

HITECH Changes to HIPAA

- Effective March 26, 2013; OCR will start enforcing on September 23, 2013.
- Most significant changes include:
  - Accountability of business associates (and their business associates)
  - Clarification of trigger for breach notification
  - Patient right to restrict data sharing with payers (POOP)
  - Patient rights to electronic data in the form or format requested (and to have data directly transmitted to others)
- Changes to Accounting of Disclosure rules/proposed access report still in development (probably another proposed rule)

Busting myths about HIPAA

- HIPAA Privacy Rule myths persist
- Some of the most common:
  - HIPAA prohibits data sharing, including with other providers (even for treatment) and with the patient, or with the patient's involved family members
- Fears of HIPAA "lawsuits" (HIPAA has no private right of action)
- Increased enforcement activity heightens concerns (even though details indicate that only serious failures to implement trigger fines/ settlements)
- Privacy rule permits sharing for most routine health care activities – but such sharing is rarely required

Taking Data Security Seriously

- **Results of OCR HIPAA Security Rule Audits:**
  - **58/59 providers at at least 1 security finding or observation**
  - **No complete and accurate risk assessment done in 2/3 of entities audited**
  - **Addressable implementation specifications (e.g., encryption) – entities either fully implemented or did nothing.**
- **Audits of "meaningful users" also show lack of documentation of security risk assessment**
- **Most breach reports post HITECH due to lost or stolen, unencrypted portable media**

Health Data Not Covered by HIPAA

- Bloomberg News/Latanya Sweeney report showing aggregate health data released or sold by states can be fairly easily re-identified
- Report of Privacy Rights Clearinghouse demonstrates deficiencies in 43 mobile health and fitness app data practices
  - More than 75% of the free apps and 45% of the paid apps used behavioral tracking, often through multiple third-party analytic tools.
  - Of those who share data with analytic services, only 6% of free apps and 15% of paid apps used encrypted SSL connections.
  - In majority of apps, data practices were not accurately described or frequently even mentioned in privacy policies.
- JAMA Internal Medicine research letter (7/8/13) looked at 20 health websites: 13 tracked users; 7 shared data w/outside companies.

Clinical Data Outside HIPAA Bubble Likely to Increase

- MU Stage 2:
  - Ambulatory professionals and hospitals must make information in view/download/transmit available to patients – and get 5% of them to use it.
  - Also must have 5% of patients securely e-mail.
- Not a replacement for HIPAA Privacy Rule patient access requirements – but providers can use meaningful use/CEHRT capabilities to help meet HIPAA requirements.
- Deployment of Blue Button Plus
- Patients ability to receive information through unsecure e-mail (clarified in 2013 Omnibus) – right of access trumps HIPAA Security Rule

Latest Consumer Privacy Developments

- White House report – "Consumer Privacy Bill of Rights" (Feb 2012)
  - Established Bill of Rights based on fair information practices; consent is "contextual"
  - Called on Congress to pass baseline consumer privacy legislation
  - Called for multi-stakeholder efforts to develop industry codes of conduct (industry best practices) that could be enforced by FTC for adopting companies
  - Called for increased international collaboration on data privacy regulations

Latest Consumer Privacy Developments

- FTC final report (March 2012)
  - Articulated privacy framework based on fair information practices; contextual approach to consent
  - Also called on Congress to enact baseline privacy legislation
  - Praised ongoing efforts on Do-Not-Track (unclear whether these will be successful)
  - Endorsed industry codes of conduct
  - Endorsed role for U.S. in achieving harmonization of U.S.-global data privacy policies

Challenges to "Secondary" Health Data Uses

- Research rules (HIPAA, HHS) rely significantly on consent for identifiable data
- Less identifiable = less regulation
- HIPAA de-identified data not subject to limits

HIPAA & Uses of PHI for Quality Improvement

- HIPAA
  - Consent is not required to use identifiable data (PHI) for treatment, payment or "health care operations"
  - Research uses of PHI require prior authorization, unless this requirement is waived by an IRB or Privacy Board; in addition, Common Rule is likely to apply to use of clinical PHI for research purposes.
- HIPAA regulatory structure is consistent with data privacy rules that distinguish between uses of data that would be routine or reasonably expected by the data subjects versus those that are less likely to be expected

Research vs. Operations

- **HIPAA**
  - Health care operations includes "conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, ***provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities***." Also includes "population-based activities relating to improving health or reducing health care costs, and protocol development.
  - Research is a "systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."
- **Common Rule has the same definition for research.**

Paradox

- Two studies using data for quality improvement purposes: both use the same data points, are done to address the same question or sets of questions, and are done by the same institution. They will be:
  - Treated as operations if the results are only to be used internally
  - Treated as research if the intent is to share the results with others so that "learning" may occur.
- How does this advance both the learning healthcare system and protections for data?

Health IT Policy Committee (HITECH) Comments to Common Rule ANPRM

- **Use of clinical data to evaluate safety, quality and efficacy should be treated like operations, even if the intent is to share results for generalizable knowledge, as long as provider entity maintains oversight and control over data use decisions.**
- **Entities should follow the full complement of fair information practices in using PHI for these purposes.**
- **Recommendations provided some examples of activities with clinical data that should be treated as operations – but also acknowledged further work was needed to determine a new line for when analytics with EHR data should be treated under more robust rules.**

Recommendation letter of 10/18/11 - http://www.healthit.gov/policy-researchers-implementers/health-it-policy-committee-recommendations-national-coordinator-heal

Conclusion

- Health data environment is growing richer by the day
- Privacy, safety concerns persist – direction of policy efforts to address uncertain
- Will e-patient movement explode with greater health data access?
- Are current rules governing secondary uses of data really the obstacle to the learning health care system – and if so, what needs to be changed?

Questions?

Deven McGraw

202-637-9800 x133

deven@cdt.org

www.cdt.org/healthprivacy

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE