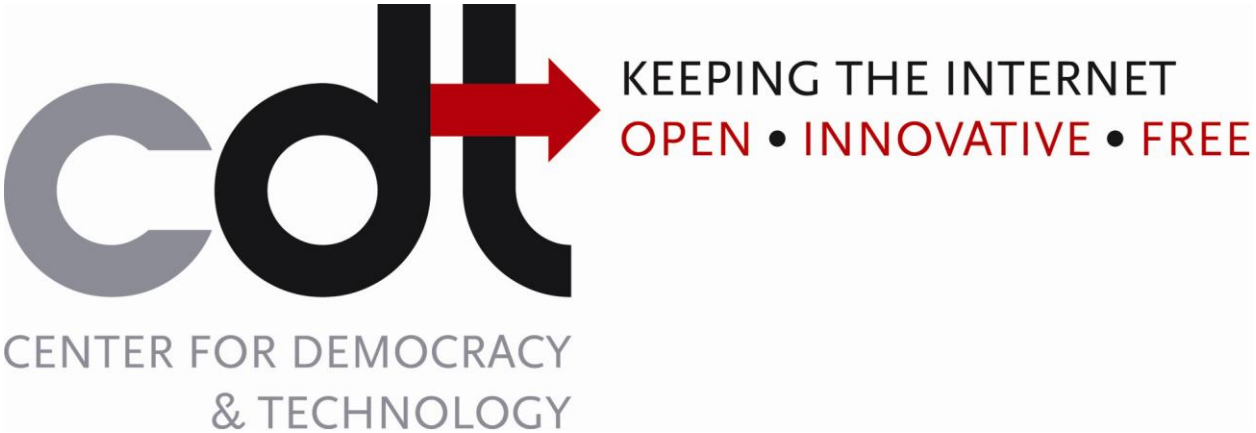

Meaningful Choice in a Learning Health Care System: the Relationship Between Privacy and Data Sharing for Research

Alice Leiter, JD
Policy Counsel, Health Privacy Project
February 26, 2013

The Health Privacy Project at CDT

- Health IT and electronic health information exchange are the engines of health reform & have tremendous potential to improve individual and population health
- Some progress has been made on resolving the privacy and security issues raised by e-health – but questions remain and implementation challenges loom
- Project's aim: Develop and promote workable (or "practical") privacy and security policy solutions for storing and sharing personal health information

Learning Healthcare System

- Drawing research closer to clinical practice by building knowledge development and application into each stage of the healthcare delivery process
- A system in which knowledge generation is so embedded into the core of the practice of medicine that it is a natural outgrowth and product of the healthcare delivery process and leads to continual improvement in care
- In order to achieve this, need to be able to safely and securely leverage clinical data for purposes beyond treatment and payment

How does HIPAA govern data uses for population health? (general overview)

- HIPAA applies only to individually identifiable health information – data that is "de-identified not subject to any regulation.
  - Legal standard: no reasonable basis to believe the data can be used to identify an individual
  - Two methodologies – safe harbor (removal of 18 specific identifiers, including dates) and statistical methodology (must achieve very small risk of re-identification)
- "Limited Data Sets" (the close cousin to de-identified data – removal of 16 categories of information) are permitted for research; data holders are required to execute data use agreements; individual consent typically not required

HIPAA & Population Health (cont.)

- Before identifiable information can be used for research purposes, must obtain patient's authorization
  - Can be waived by a Privacy Board or IRB if risk to privacy is considered to be low
  - Some exceptions (review of data onsite in preparation for research, as an example)
- Research on data that qualifies as "de-identified" is largely not regulated at all, hence enormous appeal of achieving HIPAA de-identification

Other (legal) requirements that may apply

- Most apply only to data that is identifiable or can reasonably be identified (not tied to HIPAA standards, although HHS appears to be moving in that direction for the Common Rule)
  - Common Rule (governing federally funded research)
  - State health and consumer privacy laws
  - Regulations on federally funded substance abuse treatment facilities
  - NIH rules
  - Grant conditions
  - HIE (health information exchange) rules
  - In some cases, international law may apply

The Common Rule

- Applies to research on identifiable data
- Includes health services research
- Open ANPRM proposing some fairly significant changes
  - Research on data collected for clinical purposes but secondarily used for research purposes would be exempt from requiring IRB approval – but if data are identifiable, consent is required (but general consent would suffice); one-two page registration of study with IRB/institution required
  - Rely on HIPAA for standards of identifiability
  - Require adoption of data security protections
  - Biospecimens collected for clinical purposes – requires consent for research even if not identifiable

Common Criticisms of Legal Requirements

- Focus is disproportionately on identifiability of data and whether or not consent is required
- Overemphasis of two privacy-protective tools, while (almost) completely ignoring others
- Conservative interpretation of the rules is more of a problem than the rules themselves

What does good health privacy and security look like?

- A comprehensive privacy and security framework is needed to facilitate health IT and health information exchange
- Rather than being so focused on consent, it should be based on ALL OF the fair information practices (FIPs)
- Key to incorporate notions of consumer/patient expectations – or “context” – in determining privacy protections to deploy
- This provides the foundation of meaningful choice

What does meaningful choice look like?

- Includes the ability to make the choice in advance;
- To be free to make the choice (and not be denied medical treatment based on a choice not to participate); and
- To have full transparency and education about the choice. Both "opt-in" and "opt-out" models are acceptable if the choice provided is "meaningful."

Fair Information Practices – Markle Common Framework

- Openness and transparency
- Purpose specification and minimization
- Collection limitation
- Use limitation
- Individual participation and control
- Data integrity and quality
- Security safeguards and controls
- Accountability and Oversight
- Remedies

Value of Distributed/Federated Networks for Multi-Site Research using EHRs

- Raw, identifiable data remains with data holder
  - Leverages patient trust in health care providers; addresses institution concerns about releasing “their” data
- Data standardization/normalization occurs at source
- Analytics done on original data
  - By data holder, or researcher can be granted on-site access
- Results shared
  - Either de-identified data or limited data set

Policy Advantages

- De-identified (or LDS) data that is shared with others is subject to fewer regulatory constraints under HIPAA, Common Rule, and Part 2 regulations
  - Also, most state health privacy laws apply only to identifiable data
- Participating entities must still comply with applicable law with respect to their ability to access/use information for research
- Multiplicity of state laws can be managed -- each institution need only comply the laws of its own state (e.g., does my state law permit me to use data and disclose data for this purpose; no need to consider laws of other participating states)

Questions?

Alice Leiter

202-637-9800 x120

alice@cdt.org

www.cdt.org/healthprivacy

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE