Learning as Part of "Operations": Challenges Posed By the Current Regulatory Framework

Alice Leiter
Health Privacy Project
February 24, 2014

HIPAA & Uses of PHI for Quality Improvement

- 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

- Under 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 either the learning healthcare system or 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

CDT Criticisms of Current Legal Requirements

- Focus is disproportionately on identifiability of data and whether or not consent is required
  - De-identification is an important data protection tool but it is not infallible (still very low risk of re-identification)
  - Individual consent (control) is an important component of fair information practices, but it is just one component. It tends to provide weak privacy protection in practice, as authorizations are either generally worded (and therefore not informative) or too long (and therefore not read or understood)
- Overemphasis of two fair information practice principles (FIPPs), while (almost) completely ignoring others

Challenges For Multi-Site Research Initiatives

- Current rules provide disincentive to publish or otherwise share data and study results
- “Better safe than sorry” approach
  - Uncertainty re: legal requirements leads to treatment of all data re-use as research
  - Creates real barriers given strict requirements
- Federated, or decentralized, network architectures are more privacy-protective, yet current law provides no incentives to employ such structures

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

Potential Paths Forward

- At least test different frameworks for protecting privacy in research using clinical data
  - Consider a more risk-based regulatory framework, under which (for example) publication of study results is not treated as inherently risky
  - Rely less on consent (esp. for uses of data that, in a learning health care system, should be considered “routine”) and instead pursue other models of patient engagement (e.g., input into research; greater transparency re: research uses of data; requirements to share results with patients)
  - Consider mechanisms of accountability/oversight (Canadian model (PHIPA), voluntary research network governance models, accreditation)
  - Study their efficacy in building and maintaining public trust in research.
- Research on data supplied by patients

Questions?

Alice Leiter

aleiter@cdt.org

www.cdt.org/healthprivacy