Protecting Privacy and Advancing the “Learning Health Care System”

Deven McGraw, JD, MPH, LLM
Director, Health Privacy Project
July 16, 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, through balanced & workable protections, as they are essential to health reform and building a “learning health care system.”
How does HIPAA govern analytic uses of data?

- HIPAA applies only to individually identifiable health information – data that is “de-identified” per HIPAA standards is not subject to any regulation.

- “Limited Data Sets” (the close cousin to de-identified data) are permitted for research; data holders are required to execute data use agreements; individual consent typically not required.

- We are familiar with research networks that rely on these data types – but not always ideal for all types of research.
Before fully identifiable information can be used for research purposes, the patient’s authorization must be obtained (currently authorization must be study specific – but Omnibus rule allows for authorizations for future research, as long as that future research is “sufficiently described”)

- 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, research on decedent’s info, and use of limited data set)

Scope of new rule uncertain
Uses and disclosures of identifiable health data for “health care operations” do not require individual consent or authorization.

- Includes conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines; population-based activities relating to improving health or reducing costs.
- However, if “obtaining of generalizable knowledge” is a primary purpose of these activities, it is considered “research” and not operations.
The Common Rule

- Applies to federally funded research (or research in federally funded institutions) on identifiable data; similar definition of research as in HIPAA

- Includes health services research

- Review of IRB (either full or expedited) required

- Consent required, although can be waived if:
  - The research involves no more than minimal risk
  - The waiver will not adversely affect the rights & welfare of subjects
  - The research could not be practicably conducted w/out the waiver; and
  - When appropriate, subjects are provided with additional info after participation.
The Common Rule (cont.)

- ANPRM sought comment on fairly significant changes
  - Research on data collected for clinical purposes but secondarily used for research purposes would be exempt from requiring IRB approval – one-two page registration of study with IRB/institution required instead
  - If data are identifiable, consent is required (but general consent would suffice);
  - 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

- Unclear if/when proposed rule will be issued…
Issues with Current Federal Legal Frameworks Governing Health Data Analytics

- Genuine confusion about application of the rules
- Overly conservative interpretation of the rules – in most cases, HIPAA says “can” not “must”
- Health services research often requires multiple sites to work together – typically not easy
  - Data as an asset
  - Data holders have a legal responsibility to protect; variances in risk tolerance
  - Differences in state law can also create obstacles
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?
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.

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 control is an important component of fair information practices - but it is just one component. It tends to provide weak privacy protection in practice (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 (FIPs), while (almost) completely ignoring others
- No incentives in the law to pursue privacy-protective data sharing architectures
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

- Research on data supplied by patients
- At least experiment with different frameworks for protecting privacy in research using clinical data
  - Rely less on consent 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)
  - Mechanisms of accountability/oversight (Canadian model (PHIPA), voluntary research network governance models, accreditation)
  - Incentives to pursue privacy-enhancing data sharing architectures
- Study their efficacy in building and maintaining public trust in research.
Questions?

Deven McGraw
202-637-9800 x115
deven@cdt.org
www.cdt.org/healthprivacy