manatt

HIPAA and the Learning Health System

Balancing the Risks and Benefits of the Digital Healthcare Revolution

Deven McGraw, JD, MPH, LLM
Partner
Manatt, Phelps & Phillips, LLP

December 10, 2014

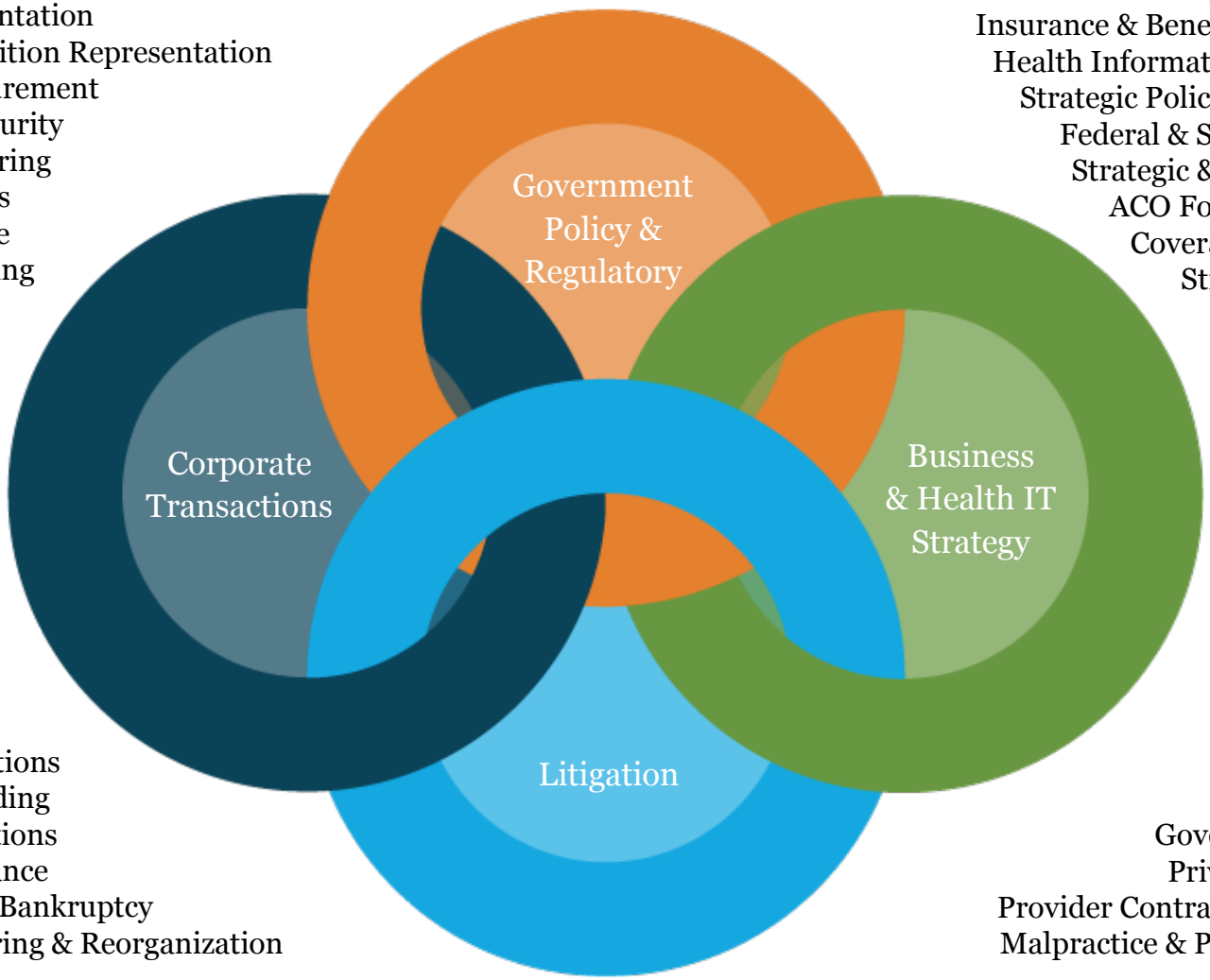
Our mission is to be a practice whose multidisciplinary professionals, through excellence, deep substantive knowledge and teamwork, support clients seeking to transform America's health system by expanding coverage, increasing access and creating new ways of organizing, paying for and delivering care.

- Interdisciplinary team with over 80 professionals
- Pharmaceutical strategy: health reform, pricing, Medicare reimbursement, regulation of research, approval, manufacturing and marketing of medicines
- Provider strategy: IDNs, academic medical centers, children's health, ACO formation
- Privacy and security
- Mergers, acquisitions, joint ventures
- Corporate structure and governance
- Medicaid program evaluation and redesign
- Payer strategy: provider-sponsored plans
- Health information exchange, health IT
- Insurance

Manatt Health: Interdisciplinary Services

Congressional, Federal & State
Agency Representation
Association & Coalition Representation
Government Procurement
Data Privacy & Security
Legislative Monitoring
Legislative Analysis
HIPAA Compliance
Language Drafting
Reimbursement
Fraud & Abuse
Lobbying

Healthcare Financing & Reimbursement
Insurance & Benefit Exchange Design
Health Information Exchange (HIE)
Strategic Policy & Market Analysis
Federal & State Policy Advisory
Strategic & Financial Planning
ACO Formation & Planning
Coverage & Access Design
Strategic Partnerships
Health IT Strategy
Business Strategy



Contracts
Antitrust
Compliance
Accreditation
Joint Ventures
Tax Exemption
Corporate Finance
Mergers & Acquisitions
Investment & Funding
Physician Transactions
Nonprofit Governance
Credit Recovery & Bankruptcy
Corporate Structuring & Reorganization

Real Estate
Knox-Keene
False Claims
Investigations
Reimbursement
Creditors' Rights
Fiduciary Liability
Contract Disputes
Unfair Competition
Government Regulation
Privacy & Ethics Issues
Provider Contracting Arrangements
Malpractice & Professional Liability

Health Data Gets Big (or at Least Bigger)

- Increased adoption of electronic medical records by healthcare providers
- Increased sharing of electronic and claims data with patients (and increasing flows of patient-generated information back)
- Explosion of health and medical apps, social networking sites
- Establishment of all-payer claims databases
- Payment reform driving increased reliance on analytics:
  - Accountable Care Organizations
  - Predictive Analytics
  - Patient-Centered Medical Homes
- Free the Data initiatives (including Medicare)
- PCORNet (11 Clinical Data Research Networks and 18 Patient-Powered Research Networks)
- Efforts launched to enable reexamination of information collected for clinical trials

Health Big Data Challenges

- Need trusted ecosystem
  - Privacy, confidentiality and security
  - Data governance
- Insufficient incentives to share information and invest in analytics, particularly across multiple, often competing organizations and institutions
- Interoperability still elusive goal
- Data quality

How Does HIPAA Govern Analytic Uses of Data?

- De-identified data ≠ PHI, not subject to HIPAA
- "Limited Data Sets" = PHI, but less regulated by HIPAA
- Heavy reliance on these two models – but not ideal for all types of analytics
- Questions raised about de-identification as reliable tool for privacy-protected health data analytics
  - Concerns about greater re-identification risks
  - Limited Data Set at least has requirement for Data Use Agreement

Heavy Reliance on Consent for HIPAA (and Common Rule)

- HIPAA – consent for "research" using PHI is generally required unless waived by a Privacy Board or IRB
  - – Exemptions for "prep to research" activities and research using decedent's info
  - – Waiver criteria:
    - Adequate plan to protect identifiers from improper use and disclosure (destroy after research)
    - Adequate written assurances that information will not be reused or disclosed to any other person/entity
    - Research could not practicably be conducted without the waiver or without the access to the information.
- The Common Rule – consent for "research" using identifiable information is required unless waived by an IRB
  - Research involves no more than minimal risk and research will not adversely affect rights and welfare of subjects
  - Research could not practicably be conducted without the waiver
  - When appropriate, subjects provided with additional information after participation

Are Regulatory Changes Sufficient? HIPAA

- Use of fully identifiable PHI for research generally requires prior patient authorization
  - Historically required to be study-specific
- Omnibus rule (January 2013) now allows for authorizations for future research, as long as that future research is “sufficiently described”)
- Scope of new rule uncertain

The Common Rule

- Advance Notice of Proposed Rulemaking in 2011 (http://www.hhs.gov/ohrp/humansubjects/anprm2011page.html) 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
- Release of proposed rule uncertain

Standard of Care Research – Draft Guidance

- October 2014, Office of Human Research Protections issues draft guidance on "Standard of Care" research (http://www.hhs.gov/ohrp/newsroom/rfc/comstdofcare.html)
- "Standard of Care" research evaluates treatments recognized and used in practice but where there is insufficient evidence re which works best and in which population(s)
- Under Common Rule, role of IRB is to evaluate the risks and benefits of **research** (distinct from what a person would otherwise experience)
  - Guidance concludes that randomization of individuals in a study involves research risk, because the care an individual receives will be different than what they would have received but for the research
  - Reviews of clinical data do not introduce additional risks
- Comments due December 23, 2014 (http://www.gpo.gov/fdsys/pkg/FR-2014-10-24/html/2014-25318.htm)

Research vs. Operations

- HIPAA
  - Healthcare 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" (emphasis added). 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 intended to be used internally
  - Treated as research if a primary purpose is to share the results with others so that “learning” may occur
  - Guidance on “primary purpose” allows for a later change in plans – but initially you have to intend to be doing only operations
- 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

Fixing the Paradox?

- Modify HIPAA regulations for data reuse so that regulations more directly address privacy and confidentiality risks.
  - Potentially could also do through waiver guidance
- Impose greater regulation of reuses of data that present greater risk to privacy, confidentiality and security. What factors trigger greater risk?
  - Where is the data analyzed (internal vs. external, physical location vs. control)?
  - Sensitivity of the data (type of data, vulnerable populations)
  - Failure to establish and adhere to FIPPs-based policies
    - Transparency
    - Data minimization ("minimum necessary"), collection and use limitations
    - Security safeguards
    - Accountability and oversight

Fixing the Paradox?

- Guidance with respect to the distinction between operations and research – and/or when waivers can be granted
- Experiment (federal HIPAA waivers?) to test with different models for protecting privacy in research
  - 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
Partner
Manatt, Phelps & Phillips, LLP
dmcgraw@manatt.com

UPMC LIFE CHANGING MEDICINE

The HIPAA Paradox

John Houston

Learning Healthcare Systems

- The Institute of Medicine describes a learning health care system, as a health system in which care of patients is integrated with medical research so that the health care practices offered in the system are continuously studied and improved.
- Research influences practice and practice influences research.
- One key element of a learning healthcare systems is the concept of advancing clinical data as a public utility.

Belmont Report Perspective

- Human subject “protection from harm” is a primary concern of during the research endeavor.
- Human subject’s privacy is a research protection that must be respected, resulting in the requirement for patient consent.
- Should this fundamental human subject protection extend to other similar non-research related re-uses that may be fall under “Healthcare Operations”?

NLM/NIH Preference Consent Study

2003 NLM / NIH Study titled "**Patients' consent preferences for research uses of information in electronic medical records: interview and survey data**"

- The objective was "To assess patients' preferred method of consent for the use of information from electronic medical records for research"
- Most interviewees were willing to allow the use of their information for research purposes, although the majority preferred that consent was sought first. The seeking of consent was considered an important element of respect for the individual.
- Most interviewees made little distinction between identifiable and anonymised data.
- Research sponsored by private insurance firms generated the greatest concern, and research sponsored by foundation the least.
- Sponsorship by drug companies evoked negative responses during interview and positive responses in the survey.

UPMC LIFE CHANGING MEDICINE

Considerations

- Is the advancement of a learning healthcare system “research” or is it “healthcare operations”? And, practically, does it matter?
- In the definition of “healthcare operations”, are the ”development of clinical guidelines” and “protocol development” equivalent to obtaining “generalizable knowledge”?
- If so, then why is there a distinction with respect to consent?

Considerations

- Does retrospective research involving data warrant the same privacy protections, especially where the development a learning healthcare system is the motivation?
- How should the use of data that is necessary for IT Development be addressed?
- Is “risk” the proper variable to determine when consent is required? Or, should the standard align with patient expectations or some assessment of societal value?

Example - Contracts of Adhesion

- Many accrediting bodies and vendors require that they have the right to re-use data, often as a limited data set for unrelated and unspecified purposes.
- The covered entity often has no oversight or ability to control what those uses are, yet are required to agree to the right in order to receive the accreditation or service.