EPSTEIN
BECKER
GREEN

Consumer-Driven Health Data Sharing:
Legal and Regulatory Landscape

By Alaap Shah, JD MPH

August 28, 2019

eHealth Initiative

Privacy and Security Task Force

Presented by

Alaap B. Shah

Member of the Firm

Epstein Becker Green P.C.

ABShah@ebglaw.com

202.861.5320

My Background

- Member of the Firm, Epstein Becker & Green P.C.
  - Partner in Heath Care and Life Sciences Division
  - Co-Lead of Data Privacy, Cybersecurity and Data Asset Management Team
- American Society of Clinical Oncology/CancerLinQ
  - Senior Counsel, Chief Privacy and Security Officer
  - Helped launch CancerLinQ – Big Data in Oncology
  - Helped manage enterprise-wide risk associated with privacy and security
- Certified by IAPP as a Privacy Professional
- Certified by HIMSS as a Health Information Systems Professional
- Certified by HITRUST on the Common Security Framework

Today's Agenda

- HIPAA's Role in Consumer Direct Health
- FTC's Role in Consumer Direct Health
- State Law Developments
- ONC Proposed Rules on Interoperability
- Need for Regulatory Harmonization?

AI Market: Data is King

The world's most valuable resource is no longer oil, but data.

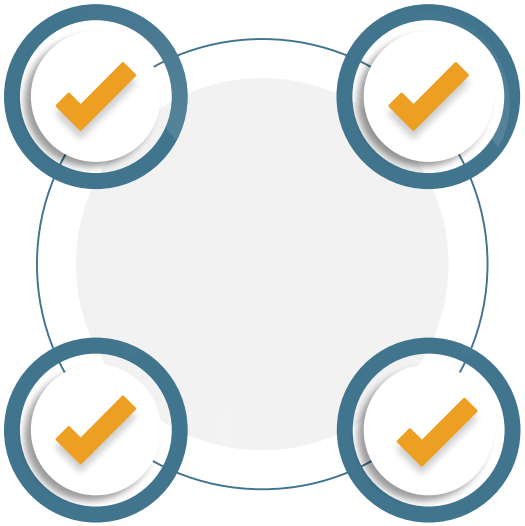
- *"Alphabet, Amazon, Apple, Facebook and Microsoft . . . are the five most valuable listed firms in the world."*
- *"With data there are extra network effects. By collecting more data, a firm has more scope to improve its products, which attract more users, generating even more data, and so on."*
- *"They have a 'God's eye view' of activities in their own markets and beyond."*

The 'Data Economy' is at a fever pitch. Enormous value may be realized as long as data continues to flow and trust is maintained.

Credit: The Economist, May 6, 2017

HIPAA In a Nutshell…

The Privacy Rule regulates use or disclose of Protected Health Information ("PHI") and obligations to subjects of that information.



The Breach Notification Rule establishes obligations to report security incidents and breaches to various stakeholders

The Security Rule sets standards to protect the availability, integrity, and confidentiality of E-PHI

The Enforcement Rule establishes the penalty framework for HIPAA violations

Who is Subject to HIPAA?

Covered Entities	Business Associates

• **Health care providers:** providers of medical or health services who transmit health information in electronic form
 	
• **Health plans:**
  • Health insurers and HMOs
  • Insured and self-funded employee welfare benefit plans that have 50 or more participants or are administered by an entity other than the sponsor
 	
• **Health care clearinghouses:** billing services, re-pricing companies and others that engage in data translation
	• Performing functions or provides services involving PHI or maintains PHI on behalf of a Covered Entity
	
	• Broad scope of entities considered BAs
	
	• Examples:
	  • Cloud or software vendor who hosts software containing PHI
	  • Data analytics involving PHI
	  • Vendor support involving PHI
	  • Revenue cycle management
	  • Patient outreach activities
	  • Utilization review
	  • Quality Assurance
	  • Benefits management
	  • Legal/Accounting services

HIPAA's Role in Consumer Directed Health

- Recent OCR FAQ guidance:
  - Individuals have right to access PHI (including transmission to a third party app)
    - Cannot deny request based on concerns about app privacy or security
  - Apps developed for or on behalf of a Covered Entity by a Business Associate will likely be covered by HIPAA
    - BAA required
    - Subsequent use and disclosure of PHI will be subject to HIPAA
  - Covered Entities that transmit PHI to a non-HIPAA covered apps will not be liable for subsequent unlawful uses or disclosure of that data
    - Terms of use and privacy policy of third party app will govern.
    - Transmission of PHI may be unsecured if requested by an individual as long as risks are explained to the individual

FTC's Role in Consumer Directed Health

- Section 5 of the FTC Act
  - Prohibits unfair methods of competition
  - Section 5(n) provides the standard for "unfairness"
    - If and act "causes or is likely to cause substantial injury to consumers"; the injury to be caused "is not reasonably avoidable by consumers themselves"; and the injury is "not outweighed by countervailing benefits to consumers or competition."
  - FTC actions have been based on:
    - Failure to safeguard information;
    - Failure to adequately disclose to consumers how information will be used or disclosed;
    - Misrepresenting how information collected would be used

FTC's Role in Consumer Directed Health

- FTC Privacy Expectations
  - Build privacy considerations in from the start
  - Be transparent about data practices
  - Offer choices that are easy to find and easy to use
  - Honor privacy promises
  - Protect kids' privacy
  - Collect sensitive information only with consent
  - Keep user data secure

States' Authority: Data Security and Breach Notification Laws

- All 50 States (and the District of Columbia) have data breach notification and/or data security laws.
  - Some expressly mandate reasonable data security measures to prevent unauthorized use or disclosure.
  - All require timely **notice of breach to consumers** – with certain exceptions.
  - Some require **notice to the State Attorney General.**
  - Some require notice to credit reporting agencies.
    - *Tex. Bus. & Com. Code § 521.053(h)*
  - Some regulate the contents of a notice.
    - *N.C. Gen. Stat. Ann. § 75-65* (requiring notice of breach to be "clear and conspicuous" and in one of the methods proscribed by the statute.)
  - Some require credit monitoring.
    - *Cal. Civil Code § 1798.82(d)(2)(G)* (requiring 12 months of "appropriate identity theft prevention and mitigation services.")
    - *Conn. Gen. Stat. Ann. § 36a-701b* (requiring minimum 12 months of "appropriate identity theft protection, and, if applicable "mitigation services.")

State Law Changes and Trends

- Trends in changes to breach notification and data security laws:
  - Expanding the universe of the type of data which must be protected and which triggers notification requirement to consumers in the event of breach
    - E.g. Medical information, health insurance information, biometrics
  - Adding stricter and shorter deadlines for providing notice
  - Requiring notice to the state attorney general
  - Prescriptive requirements regarding the contents of a notice to consumers AND regarding reasonable safeguards required to protect consumer information
  - Requiring free credit reporting to affected individuals

California Consumer Privacy Act of 2018

- Effective January 1, 2020
- Requires a business that collects personal information from California consumers to disclose upon request:
  - Categories of personal information it collects;
  - The categories of sources from which it collects personal information;
  - The business or commercial purpose for collecting or selling personal information;
  - The categories of third parties with whom it shares personal information;
  - The specific personal information collected on the requesting consumer.
- Covered entities (under the Privacy Rule) are exempted

California Consumer Privacy Act of 2018

- Consumer has a right to request deletion of any personal information collected unless needed to:
  - Complete the transaction
  - Detect security incidents or to identify and debug errors
  - Exercise free speech
  - Comply with laws or legal obligations
  - Use internally consistent with context in which received information
- Consumer has right to direct business not to sell personal information ("opt out")
- Special protections for those under 16

ONC Proposed Rules on Interoperability

- Proposed Rule issued on March 4, 2019 (pursuant to 21st Century Cures Act)
  - Implement EHR conditions of certification
  - Prohibit Information Blocking
  - Prohibit Gag Clauses in EHR contracting
  - Require EHRs to publish APIs and limit fees
- Comment Period closed on June 3, 2019 (2013 comments received)
- CMS issued companion Proposed Rule governing Medicare Advantage, state Medicaid and Children's Health Insurance Program ("CHIP") Fee for Service programs, Medicaid Managed Care Plans, CHIP managed care entities, and Qualified Health Plan ("QHP") issuers in federally facilitated exchanges
- Proposed Rules geared toward promoting patient access and consumer-directed sharing of data to spur digital health innovation

ONC Proposed Rules on Interoperability

- Concerns with Proposed Rule raised throughout Comments
  - Scope of definition of Electronic Health Information (EHI) is too broad
  - Compliance with Information Blocking provisions may be costly, complex and unduly burdensome
  - More clarity around Information Blocking exceptions is needed
  - Lack of unique patient identifier may cause patient matching issues
  - Significant gaps in privacy and security regulation for third party apps
    - All 5 former ONC Coordinators point out this issue in a joint letter

➢ Given lack of privacy and security regulation of third party apps, patients essentially are faced with the dilemma of trading away privacy rights in order to facilitate access to data.

Need for Regulatory Harmonization?

- Significant variability in data breach notification laws
- Lack of privacy and security regulation in third party app space
- Different legal and regulatory requirements for patient data depending on what entity is processing the data
- Some states have begun to adopt more sweeping privacy legislation, but this will continue to foster a fragmented legal landscape
- The Federal Government is considering legislation
  - Feb 27, 2019 – Senate Hearing on Federal Data Privacy Framework
  - Protecting Personal Health Data Act – S. 1842 (2019)
  - Privacy Bill of Rights Act – S. 1214 (2019)
  - The Information Transparency and Personal Data Control Act – H.R. 2013 (2019)