The Path Towards a New and Complete Consumer Health Privacy and Security Regulatory Structure

Kirk J. Nahra
Wiley Rein LLP
Washington, D.C.
202.719.7335
KNahra@wileyrein.com
@kirkjnahrawork

(March 28, 2018)

Today

- Quick discussion of HIPAA gaps and why they matter more each day
- The environment today – where we know the answers and where we do not
- Potential options and strategy going forward

HIPAA reminder

- HIPAA has always been a limited scope privacy/security rule – not all health information
- It applies to healthcare information only where a covered entity is involved.
- Accordingly, there always have been gaps where various entities collect or maintain health care data but are not covered by the HIPAA rules.

IoT and Unregulated Data

- Increasing concerns about big data environment
- Previous administration had been giving thoughtful and ongoing consideration to pros and cons of big data environment
- Those activities seem to have stopped for the time being

The biggest “next generation” issue

- What is “outside” of HIPAA is growing
- Web sites gather and distribute healthcare information without the involvement of a covered entity.
- These range from commercial web sites (e.g., Web MD) to patient support groups to the growth of personal health records.
- Now add mobile apps. and wearables

More “next generation” issues

- An emerging (and related) issue - bringing “outside” HIPAA information “inside” HIPAA
- CEs are gathering all kinds of data about their patients/customers/insureds from outside the health care system and using it for “health care purposes”

Recent Headlines

"Your Doctor Knows You're Killing Yourself. The Data Brokers Told Her." (Bloomberg)

- "You may soon get a call from your doctor if you've let your gym membership lapse, made a habit of picking up candy bars at the check-out counter or begin shopping at plus-sized stores."

Recent Headlines

"When a Health Plan Knows How You Shop." (New York Times)

- Health plan prediction models using consumer data from data brokers (e.g., income, marital status, number of cars), to predict emergency room use and urgent care.

The Reaction

- It is clear that there is significant concern, from the Federal Trade Commission, privacy advocates and others, about how this “non-HIPAA” health data is regulated.
- (former) FTC Commissioner Julie Brill in a (relatively) recent speech - “Big picture, consumer generated health information is proliferating, not just on the web but also through connected devices and the internet of things.”

FTC

- More from Julie Brill - this development involves “health data flows that are occurring outside of HIPAA and outside of any medical context, and therefore outside of any regulatory regime that focuses specifically on health information.”

More from the FTC

Commissioner Brill (from a recent speech)

- Then the question becomes, though, if we do have a law that protects health information but only in certain contexts, and then the same type of information or something very close to it is flowing outside of those silos that were created a long time ago, what does that mean? Are we comfortable with it? And should we be breaking down the legal silos to better protect that same health information when it is generated elsewhere.

White House Big Data Report

- A significant finding of this report is that big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace.
- The privacy frameworks that currently cover information now used in healthcare may not be well suited to address these developments or facilitate the research that drives them.

Patient Tensions

- "Patient engagement" is an important theme of health care reform
- Increased concern about how patients view use of data by entities both in and out of HIPAA
- Are there meaningful ways for patients to understand how their data is being used?

Patient Interests

- Complexity of the regulatory structure (where protections depend on sources of data rather than "kind" of data), and the difficulty of determining data sources (which is often difficult, if not impossible, to determine), has led to an increased call for broader but simplified regulation of healthcare data overall.
- This likely will call into question the lines that were drawn by the HIPAA statute, and easily could lead to a re-evaluation of the overall HIPAA framework.

Tentative Predictions

- This HIPAA/non-HIPAA issue is not going away (although we may be on hiatus now)
- There is too much data being used by too many people in too many risky contexts
- Lots of pressure from many fronts to “do something” about this non-HIPAA health care data

Tentative Predictions

- 3 Main Options
- Something specific for this non-HIPAA health care data
- Something that covers all health care data (a "general" HIPAA)
- A broader overall privacy law (with or without a HIPAA carve-out)

Acting Today

- Primary challenge for companies today is how best to act in the absence of effective rules
- What do you do if no one is watching? Important role for privacy officers.
- (but some people are watching anyways – Plaintiffs' bar, state AGs, media, etc)
- Gathering now to maybe use later is an issue
- Global rules also present challenges

Acting Today

- Know what you are actually doing
- Be appropriately transparent about what you are doing
- Make sure your security is reasonable
- Be a participant in the public debate
- Be smart and responsible in your data practices

Questions?

- Kirk J. Nahra
  Wiley Rein LLP
  202.719.7335
  Knahra@wileyrein.com
  @kirkjnahrawork