What's Next for Health Care Privacy and Security?

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

(March 22, 2016)

My Presentation

- Address some of the key hot topics for privacy and security in 2016
- Start with “inside HIPAA” issues
- Move to issues that are “partially HIPAA,” even if driven by other rules/laws
- And then conclude with what’s “next to” HIPAA

Inside HIPAA - OCR Enforcement Changes

- Despite press reports every time there is a new case, no meaningful increase to date
- Investigations are more thorough and more burdensome
- Increasing pressure to do more on both audits and investigations
- Still generally very reasonable

Enforcement

- Cases involving significant failures of compliance
- Cases involving repeated and/or uncorrected problems
- Particularly “noticeable” problems
- High impact cases (?)

Enforcement

- There is pressure to do more
- Note – Many of the biggest breaches have not resulted in enforcement (yet)
- Remember – A security breach does not mean a HIPAA violation
- How does the FTC fit into any enforcement pressure?

Enforcement - Business Associates

- Now subject to full HIPAA enforcement regime
- Many BAs are not in reasonable compliance with HIPAA Security Rule, particularly on documentation
- Is it fair to think they would be?
- Little consistency across BA universe

Business Associates

- No real enforcement involving business associates yet
- A real challenge for OCR – how to treat companies who deal with much more than health care
- And the enormous range of size/sophistication of these entities
- Enormous variations in actual contact with PHI

Enforcement – Audits

- Will we finally see the Phase 2 audit program in 2016?
- What is the goal of this program?
- We can expect that covered entities will do reasonably well on the Privacy Rule and not as well (and maybe badly) on the Security Rule
- BAs – if included – likely will be bad at all of it.

Partially HIPAA

- Potential new legislation – 21st Century Cures
- Major legislation, with small number of privacy provisions (receiving almost no attention)
- Current provisions could dramatically change research rules
- Also could allow pharma to buy PHI for “research” or “public health” without payment limits
- Will this open up HIPAA again?

Partially HIPAA

- Mental Health/Substance Abuse – potential revisions to federal substance abuse rules, to bring them closer (but not really close) to rest of the HIPAA Structure
- Common Rule revisions, with significant privacy implications

Next to HIPAA

- What is “outside” of HIPAA is growing
- Web sites gather and distribute healthcare information - ranging from commercial web sites (e.g., Web MD) to patient support groups.
- Significant expansion of mobile applications directed to healthcare data or offered in connection with health information
- “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

- 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.”
- 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.
- Fortune - Employers Are Quietly Using Big Data to Track Employee Pregnancies.

What's Next?

- The debate about "non-HIPAA" healthcare data is not going away
- Lots of pressure from many fronts to "do something" about this non-HIPAA health care data
- There is too much data being used by too many people in too many risky contexts
- Therefore . . .

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)

Questions?

For further information, contact:

- Kirk J. Nahra

  Wiley Rein LLP

  202.719.7335

  Knahra@wileyrein.com

  @kirkjnahrawork

- Subscribe (for free) to *Privacy in Focus* - http://www.wileyrein.com/publications.cfm?sp=newsletters