Looking Over the Rainbow: What's Next in Legislation and Policy Impacting Health Privacy & Security

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

(May 22, 2013)

My Presentation

- Obviously, everyone is still digesting the omnibus regulation
- And it's not even subject to compliance yet
- But, between the passage of time and the overall movement of the health care industry, what's happening next on health care privacy and security?
- This session will identify and discuss some upcoming regulatory developments and some issues that need tackling

Immediate Term - Compliance

- Figure out how to deal with breaches (use the compliance period to compare the two standards and the results)
- Develop a plan for business associate contracts
- Deal with the HIPAA Security Rule (mainly for BAs)
- Identify sale and marketing complications

Next Issues - Regulatory

- The HIPAA Accounting Rule
- A significant holdover from HITECH
- Separate NPRM addressing the HITECH language on the accounting rule – not part of the "big" HITECH Rule
- A slower timetable (some of us hope for indefinite delay)

The Accounting NPRM

- Remember the HITECH Language – TPO exception to the accounting obligation would not exist for “disclosures” “through an EHR.”
- We expected a rule that limited the scope of “through an EHR” and connected to EHR technology
- Instead, NPRM broadly implements this requirement and expands (substantially) through general HIPAA authority

The Accounting NPRM

- Lots of comments were submitted, essentially all of them highly critical of the NPRM
- Virtually no one supported the proposed rule
- *Implications for now* - *Important to evaluate what your company actually does with audit logs and similar oversight efforts. Do not start building an access report.*
- You will need to have a plan for this issue.

The Accounting Rule

- Big question – Is this a fundamental change in approach or something else?
- Will the accounting rule become a major compliance and financial challenge?
- How is this consistent with the Administration's effort to streamline regulations?
- Is this a big change in the balance between patient interests and compliance burden?

Other Issues - Regulatory

- "Minimum necessary" – Guidance is promised at some point
- This is really hard to do on a general level – the challenge is to try to tell an entire industry how to act in the same way
- Expect some guidance on process more than substance

Other issues - Regulatory

- Is there anything else that should be done to the HIPAA Rules?
- OCR indicated that it would look beyond HITECH (but then didn't do too much here)
- Are there appropriate "fixes" to HIPAA (and in which direction?) (e.g., privacy notices)

Other Issues - Regulatory

- De-Identification
- Some guidance already (mainly for technical folks)
- Will there be more coming?
- Attention being paid to “big data” and new technology (along with money to be made) will keep attention on this issue.

Security Practices

- The omnibus regulation had no material changes to the security rule (other than application to business associates)
- That means that this rule hasn't changed in almost ten years.
- Security breaches remain an enormous problem.

Security Practices

- Expect significant pressure to implement "tougher" security standards
- Expect real pressure for broader encryption
- Expect enforcement and adverse notice publicity to put real pressure on better practices
- Watch Congress on cybersecurity and data security link

Mobile Devices

- Enormous movement in development of mobile devices in all industries - with health care at the forefront
- FTC reviewing mobile device universe – very concerned, looking at aggressive action
- The FTC's actions will affect health care – just not clear how much

Mobile Devices/Patients

- Mobile device debate highlights tensions with role of patients in their own health care
- Ongoing questions about when "patient engagement" can be done (1) consistent with HIPAA standards or (2) without the need for HIPAA standards
- E-mail with patients as an example

A Broader HIPAA?

- Mobile device debate highlights “limits” of HIPAA
- Idea of “covered entities” and “business associates” misses whole segments of health care industry that are consumer directed or otherwise outside of HIPAA
- More attention being paid to this gap

Legislation

- Will health care get wrapped into broader legislation?
- Specialty legislation (Sen. Franken and others)
- Add-ons to HIPAA correction legislation?
- Add-ons to cyber-security?
- Add-ons (or carved out) from data security and breach notification legislation?

Litigation

- Very interesting case involving Wyndham Hotel's challenge to FTC authority to enforce general security standards.
- FTC enforces where companies fail to take reasonable and appropriate steps to protect information
- If this authority is eliminated, higher likelihood of Congress intervening.

Health Information Exchanges

- The HIE movement is proceeding largely outside of the core HIPAA discussion
- HIEs have been bogged down in privacy/security debates (and business model searches)
- State law is the issue more than HIPAA
- Is there any reasonable fix in sight?

Health Insurance Exchanges

- Critical to health care reform efforts
- Sometimes in, and sometimes outside of HIPAA
- Separate privacy and security rules, determined by each Exchange
- What is driving the differences? Do these differences matter less than with information exchanges?

Research Efforts

- Lots of opportunities for research with new data
- Some assistance from new HIPAA rules
- Some cut-backs from sale/marketing limits
- Where will the desire for research efforts and data turn next?

International Impact?

- International privacy rules are already much more restrictive on patient/individual privacy
- All health care data given “sensitive” treatment in many countries
- EU re-evaluation may make this problem even worse

Conclusions

- Lots happening, both in and out of HIPAA
- Companies need to be thinking about a lot more than HIPAA
- Will there be a convergence (a) through a broader HIPAA or (b) health care data being covered through other vehicles?
- Is this good or bad? And for whom?

Questions?

- For further information, contact:
- Kirk J. Nahra

  Wiley Rein LLP

  202.719.7335

  knahra@wileyrein.com

  @kirkjnahrawork