Preparing for and Responding to an OCR Privacy and Security Audit

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

(March 17, 2015)

My Presentation Today

- Lots happening in the world of health care privacy and security
- While many companies are still settling in to the new HIPAA environment, HHS OCR is (slowly) gearing up for the next phase of the HIPAA audit program
- We'll talk about what you might see and what you should be doing now to prepare

HIPAA Audits

- First audit program (2011-2012) was expensive and time consuming and produced a limited range of general information about the industry
- 115 comprehensive audits of Covered Entities
- HHS has been spending a long time developing the next round
- Real/reliable details on new program remain scarce

Phase 1 conclusions

- Was this worth it?
- Some limited findings published
- Not a lot of useful guidance
- Time consuming, burdensome, somewhat robotic
- Open question of cost/benefit

Next Phase of HIPAA Audits

- Expect a somewhat less intrusive model
- Starting with desk audits
- “will be an important compliance tool for OCR.”
- Mainly to generate industry information and develop technical assistance, but enforcement remains a possibility
- Very document intensive
- Role for business associates is very unclear

Next Phase of HIPAA Audits

- Will cover a mix of categories of covered entities
- Will cover business associates to some extent, but this is very much under review
- Timing remains open – should start somewhat soon, but missed some earlier stated deadlines

OCR Changes

- Where is OCR going with enforcement?
- No noticeable increase to date
- Investigations are more thorough and more burdensome
- Increasing pressure to do more on both audits and investigations

What To Watch For On Enforcement

- Change in leadership at OCR
- Enforcement approach to date has been thoughtful and reasonable
- Their approach has been consistent so far – watch for key changes
- Will the FTC put pressure on OCR to do more?

Why Prepare?

- An audit will cover much of the same territory as an investigation
- An investigation can happen at any time to anyone
- The documentation that is needed for an audit or an investigation is extensive and takes time to prepare – you can't do it on the fly (may only have 2 weeks to respond)

Responding

- Be thoughtful and responsive
- Timeliness is important
- Remember – enforcement (from an audit) is possible, but unlikely
- If you have materials to share, lean towards sharing
- This isn't the fraud people – OCR has historically been reasonable and responsible.

Security Elements

- There is real pressure to implement “tougher” security standards
- Real pressure for broader encryption
- Both CEs and your BAs have exposure in this area.
- Pay close attention to problems faced by others – through enforcement, media reports and otherwise.
- OCR cares a lot now about security - a real issue, particularly for business associates

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

Predictions

- Business Associates will look terrible as a result of these audits
- HHS will struggle with how to make sense of the business associate results, across an incredibly wide variety of BAs

Predictions

- Covered entities will fare better, but not great
- Small likelihood of enforcement, unless an entity has made no reasonable effort to comply
- Beyond that, challenge will be to produce useful results for the industry

Hints

- Take care of the easy things
- Amazing how often OCR reports “frequent problems” that seem so easy – e.g., privacy notices, patient access to records.
- Encrypt anywhere you can
- Do a better job on security generally
- Respond to complaints aggressively

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