When the Rubber meets the Road

Kirk J. Nahra
Wiley Rein LLP
Washington, DC 20006
202.719.7335
KNahra@wileyrein.com
@kirkjnahrawork

(November 17, 2015)

My Presentation

• You’ve prepared, and planned, and secured
• But now you’ve had a “breach”
• We will walk through what you do, how you think about the situation, what your key steps are and how you should investigate and resolve
• And answer your questions/hear your views
In the beginning

- Not a religious issue, but a core principle of how your company operates
- One key issue is speed
- Perhaps the most important element for your employees – where do they go when there is a potential problem?

In the beginning

- Another key issue – what are your instructions to your employees?
- How fast?
- What steps (if any) do they take before reporting?
- Anything else immediately?
Remember journalism class?

• The 5 W’s
• Who, what, where, when, why and (sometimes) how?
• Key parts of your training and what your breach team must think about

Thought process

• What do you know now?
• What can you do now?
• What must you do next?
• Don’t let notice issues distract you from the broader investigation
Privilege

• Think about privilege right from the start
• It is not as obvious an issue as you might think
• Very difficult to do, especially with speed issues
• And you may need to demonstrate to someone what you did to investigate
• Anticipate that your documents will be read by others

Mitigation

• Mitigation involves:
  • Identifying the problem
  • Determining the cause of the problem
  • Evaluating any potential harm from the problem
  • Stopping the bleeding from the problem
  • Evaluating appropriate changes (if any)
  • Determining any other legally required steps (or appropriate business steps)
  • Does mitigation require notification to individuals?
Terminology

- Breach
- Security Incident
- “Breach”
- Privacy Breach
- Potential breach?
- Other terms?

Notice/Decision Issues

- What was your role in the breach? (principal v. agent)
- What industry are you in?
- What industry is your client/customer in?
- What is the data?
- What do your contracts say?
- How many customers/clients are impacted?
HIPAA Notification Standard

- Notification is required to the affected individuals unless the covered entity “demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment.”

HIPAA Breach Risk Assessment

- Risk assessment looks at:
- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.
Implications

- The HIPAA standard is a useful one to evaluate in any situation
- It sets out the kind of analysis that you should do generally
- You are looking at the details – as best you know them – about the overall situation.

Government issues

- HHS (HIPAA notification)
- State laws/State AGs
- FTC?
- Financial institutions?
- Others?
- Timing (formal and informal)
Media Notification

- Think about requirements (and why there are requirements), and then what makes sense
- What are you trying to accomplish?
- HIPAA Setting
- Substitute Notice
- Public relations?

Communications plan

- Do you have one?
- Short term and longer term
- Think about your audiences
Weak Points

• Upstream reporting (particularly with multiple levels or multiple paths)
• Managing this upstream process and how it can affect you is an enormous issue
• Contract provisions on indemnification/notification costs
• Always read these, always negotiate in context

Approach

• State laws are important, but always think about how you are treating the overall group
• My *presumption* is to treat everyone the same
• Be aware of reasons why this presumption may not make sense
Approach

• Always think about what you must do and what you should do
• If you do something by choice, not because you have to, think about the consequences/options/implications
• Appropriate notice means you have complied with notice laws – does not mean you won’t get sued

Approach

• Do not over-generalize
• Having a process is important
• Having a list of questions/issues for consideration is important
• Having the “answers” in advance is not
Going forward

- What changes will you make?
- Make sure you have fixed problems even if you did not have to notify
- What has your history been?
- Think about personnel, infrastructure, training
- Insurance issues?
- Keep on top of problems affecting others

Questions?

- Kirk J. Nahra, Wiley Rein LLP
- 202.719.7335
- knahra@wileyrein.com
- @kirkjnahrarwork
- Subscribe (for free) to Privacy in Focus - http://www.wileyrein.com/publications.cfm?sp=newsletters.