Turning Good Information Security Into Good HIPAA Compliance

Session # 137, February 13, 2019

Adam H. Greene, JD, MPH, FHIMSS, Partner

Davis Wright Tremaine LLP

Conflict of Interest

Adam Greene, JD, MPH, FHIMSS

Has no real or apparent conflicts of interest to report.

HIMSS19

- The Difference Between Information Security and Compliance
- OCR's Focus on Risk Analysis and Risk Management
- Expectations for Policies and Procedures
- Getting Credit for Your Good Work
- Preparing for an OCR HIPAA Audit

#HIMSS19

Learning Objectives

Develop a risk analysis and risk management that is consistent with HHS Office for Civil Rights expectations

Identify evidence of implementation of controls that can be used to respond to a regulatory investigation of HIPAA compliance

Develop policies and procedures that have the level of detail that the HHS Office for Civil Rights expects

Identify key areas of the Office for Civil Rights' interpretation of the HIPAA Security Rule that differ from standard information security practices

Prepare for an Office for Civil Rights HIPAA Security Rule audit

The Difference Between Information Security and Compliance

Security vs. Compliance

What is good information security?

Successfully safeguarding confidentiality, integrity, and availability of information.

Security vs. Compliance

What is good HIPAA compliance?
• Demonstrating conformance to legal requirements. • Bonus points: … and published guidance and the regulator's expectations.

Who Regulates the HIPAA Security Rule

2003 to 2009: Centers for Medicare & Medicaid Services

2009 to present: HHS Office for Civil Rights (OCR)

… and state attorneys general

Also: The Federal Trade Commission (if for-profit entity)

How Will OCR Review Your InfoSec Compliance

Breach notification investigation

- Focused on root cause of breach

Random audit

- Could be a focused desk audit or a comprehensive onsite audit
- Very low chance of selection – but good driver for preparation
- Historically has not led to financial enforcement

Patient Complaint (rare for InfoSec)

Whistleblower – Rare, but very high risk

OCR's Focus on Risk Analysis and Risk Management

Risk Analysis

Most likely area of OCR review during audit or investigation

Leading cause of financial settlements and penalties

Most likely disconnect between info security professionals and OCR expectations

Risk Analysis

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."

45 C.F.R. § 164.308(a)(1)(ii)(A)

Risk Assessment vs. Gap Assessment

A gap analysis is typically a narrowed examination of a covered entity or business associate's enterprise to assess whether certain controls or safeguards required by the Security Rule have been implemented. A gap analysis provides a high-level overview of how an entity's safeguards are implemented and show what is incomplete or missing (i.e., spotting "gaps"), but it generally does not provide a comprehensive, enterprise-wide view of the security processes of covered entities and business associates.

business associates to safeguard electronic protected health information (ePHI) through reasonable and appropriate security measures. One of these measures required by the Security Rule, is a risk analysis, which directs covered entities and business associates to conduct a thorough and accurate assessment of the risks and vulnerabilities to ePHI (*See* 45 CFR § 164.308(a)(1)(ii)(A)). Conducting a risk analysis assists covered entities and business associates identify and implement safeguards that ensure the

Risk Assessment vs. Gap Assessment

		Policies &	Policies &	
	policies and procedures.			
45 C.F.R. § 164.308(a)(1)(ii)(D)	**Information System Activity Review:** Implement procedures to regularly review records of information system activity.	50%	50%	Not Compliant

A gap analysis similar to the above does not incorporate the above elements of a risk analysis and may not satisfy a covered entity or business associate's risk analysis obligations under the Security Rule … the example in the table above only measures an entity's compliance with specific HIPAA regulations; it does not identify and assess risks to the entity's ePHI.

Elements of a Risk Analysis

Confirm risk element satisfies certain elements:

1. Does the scope of the analysis cover all ePHI? Can include other data too.
2. Does the analysis cover all data collection? Include where PHI is created, received, maintained, transmitted, and disposed.

Elements of a Risk Analysis

3. Does the analysis list both threats and vulnerabilities? Threats include human (both malicious and inadvertent), natural (floods, earthquakes, etc.), and environmental (power failures, liquid leakage, etc.). Vulnerabilities may include technical (e.g., lack of encryption) and non-technical (e.g., ineffective training).

4. Does the analysis assess current security controls?

Elements of a Risk Analysis

5. Does the analysis realistically assess likelihood of a threat exploiting a vulnerability?
6. Does the analysis realistically assess the impact of a threat exploiting a vulnerability?
7. Does the analysis assign a level of risk for each threat-vulnerability?
8. Has the analysis been finalized?
9. Is the analysis periodically updated?

Risk Assessment During Breach Investigation

A. Please provide complete copies of any security risk analyses that were performed to comply with 45 CFR 164.308(a)(l)(ii)(A) prior to the security breach incident.

B. Identify whether and where any of the analyses identified above identify as a risk the transfer of ePHI to personal media devices of employees and/or workforce members? If yes, what was the identified level of risk?

Text (slightly modified) from an OCR data request after a breach.

Risk Assessment During Breach Investigation

Upon review of [the] risk analysis and risk mitigation plan, OCR determined that it was not a comprehensive risk analysis as it was limited in its scope to select technology. **Specifically, the risk analysis report did not include certain critical assets, such as networks (wired, wireless, and cloud based), facilities, core IT and security infrastructure, end user and mobile devices, medical devices and instrumentation, and associated security controls (logical, physical, and environmental).** Also, it should be noted that while the risk analysis report identifies more than 366 threats and known vulnerabilities, it is based on interviews with business owners and technology administrators.

Text from an OCR closure letter.

Risk Management During Breach Investigation

[Please provide] [e]vidence of security measures that are in place to reduce the risks to e-PHI identified in the risk analysis (i.e. risk management plan and accompanying evidence). (45 C.F.R. § 164.308 (a)(1)(ii)(B). **Please be sure to submit a copy of a risk management plan associated with each risk analysis requested above.** These risk management plans should describe the security measures implemented by your organization to sufficiently reduce the risks and vulnerabilities identified in the risk analyses to a reasonable and appropriate level to comply with § 164.308(a)(l)(ii)(B). Please ensure the risk management plan states the **dates of implementation** and/or **estimated dates of completion** for each security measure. Provide **evidence of implementation** where applicable (i.e. screenshots, business associate agreements, configuration settings, photographs, etc.). Please be sure to include evidence of all implemented security measures to reduce the risk of computer theft.

Text from an OCR data request.

Sample Desk Audit Findings: Risk Analysis

> The entity did not provide adequate evidence that it has conducted accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits. The entity risk analysis failed to identify were *[sic]* all systems that creates, receives, maintains, or transmits ePHI.

Excerpt from OCR desk audit of a covered entity.

Sample Desk Audit Findings: Risk Analysis

The current conducted risk analysis and the most recent Risk Analysis contains:

- A defined scope of the locations reviewed, but it fails to identify all the entity's systems that create, transmit, or maintain ePHI.
- The documentation provided from previous calendar year demonstrates that the risk analysis has been reviewed, yet it fails to demonstrate that it has been updated on a periodic basis in response to:
  - changes in the environment and/or operations
  - security incidents
  - occurrence of a significant event.

Excerpt from OCR desk audit of a covered entity.

Consider Whether Risk Analysis Should Be Under Direction of Counsel

- In-house or outside counsel engages security consultant.
- Must be for purposes of obtaining legal counsel (e.g., ensuring risk analysis complies with HIPAA, identifying info security-related legal risks).
- Counsel can review drafts to ensure consistency with regulation and guidance (e.g., does not include unnecessary legal conclusions).
- Separate any consultant remediation recommendations from risk analysis and avoid waiving privilege on recommendations document.

Expectations for Policies and Procedures

Sample Desk Audit Findings: Risk Analysis Policy

A Risk Management Policy submitted does speak in general enterprise terms of Risk Assessment. The policy, however, fails to include:

- The purpose and scope of the risk analysis. The scope is defined as personnel rather than a review of threats and vulnerabilities to data.
- Clearly defined workforce member roles and responsibilities (in the section on risk assessment).
- Management involvement in risk analysis is not clearly defined in the policy.

Excerpt from OCR desk audit of a covered entity.

Sample Desk Audit Findings: Risk Management Policy

The entity uploaded hundreds of documents, screenshots, spreadsheets, etc. in response to providing a policy for Risk Management.…The entity has many policies and procedures in place. However, most of the policies submitted do not specify or specifically relate to the security of ePHI. Rather, the policies appear to be an attempt to comply with all standards (PCI, HITRUST, etc.), and as such appear to be melded together. A single risk management policy regarding risk to ePHI was not provided, and the combination of policies that were provided do not amount to a HIPAA-specific Risk Management policy or procedure.

Excerpt from OCR desk audit of a covered entity.

Sample Desk Audit Findings: Risk Management Policy

The Risk Management Policy submitted states in the procedure section that "[CE] shall develop and maintain a Risk Management Program to manage risk to an acceptable level." It is very generic and does not specify what the entity is doing to manage risk – it only mentions what it will or shall do….

Excerpt from OCR desk audit of a covered entity.

Sample Desk Audit Findings: Risk Management Policy

Based on this document review, it was determined that the entity does not have a policy regarding risk management that includes:

- How risk is managed.
- What is considered an acceptable level of risk based on management approval.
- The frequency of reviewing ongoing risks. The policy provided only states “continually” and does not mention on-going risks.
- The workforce members’ roles in risk management process.

Excerpt from OCR desk audit of a covered entity.

Getting Credit for Your Good Work

Documentation, Documentation, Documentation …

Q: What would be an example of proof that the risk analysis was available to the workforce members?

A: Supporting documentation should show that the entity makes appropriate documentation available to appropriate individuals or groups in order for those individuals or groups to perform their job duties with respect to implementing procedures of the security rule to which the documentation pertains. For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access.

Documentation, Documentation, Documentation …

- Evidence of implementation:
  - How will you demonstrate that corrective actions have been completed?
    E.g., workstations are all encrypted.
- Evidence of routine actions:
  - How will you demonstrate that routine actions are being taken, such as that audit logs are being regularly reviewed.

Documentation, Documentation, Documentation…

Examples:

- Completed weekly checklists that security tasks (e.g., audit log review) have been completed
- Screenshots of relevant configurations (e.g., encryption on server is enabled)
- Minutes of security matters being presented to board

Documentation, Documentation, Documentation…

Case Study (True Story):

- An encrypted laptop is stolen. A terminated IT employee files a complaint with OCR claiming that you failed to report a breach.
- Can you produce documentation evidencing when all laptops were encrypted?
- Can you produce logs demonstrating that the stolen laptop was encrypted?
- Can you provide evidence that the user could not turn off encryption on the laptop?

Preparing for an OCR HIPAA Audit

Preparing for an OCR HIPAA Audit

- Step 1 – Make sure you have a current risk analysis and risk management plan
- Step 2 – Conduct a crosswalk between policies and procedures and Security Rule provisions
- Step 3 – Review policies and procedures against HIPAA audit protocol at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

Questions

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

adamgreene@dwt.com
202.973.4213
www.linkedin.com/in/Adam-Greene-DWT
Twitter: @HipaaAdam