KRIEG DEVAULT

Insights

OCR Issues Guidance on the Performance of a HIPAA Risk Analysis v. a Gap Analysis

May 9, 2018

By: Stephanie T. Eckerle and Stacy Walton Long

In April 2018 the U.S. Department of Health and Human Services Office of Civil Rights (OCR) published guidance entitled "Risk Analyses v. Gap Analyses – What is the difference?" (the "Guidance").[1] This Guidance is extremely helpful for both covered entities and business associates on the importance of and differences between a risk analyses versus a gap analyses. HIPAA requires all covered entities to undertake risk assessments to analyze the risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (ePHI).[2] This Guidance serves as an important tool and warning to covered entities that OCR not only wants to ensure that covered entities are undertaking risk assessments, but that those risk assessments are accurate, thorough, well documented and regularly updated.

In the Guidance, OCR describes the differing purposes between a risk analysis versus a gap analysis as follows:

> A risk analysis is a comprehensive evaluation of a covered entity or business associate's enterprise to identify the ePHI and the risks and vulnerabilities to the ePHI. The risk analysis is then used to make appropriate modifications to the ePHI system to reduce these risks to a reasonable and appropriate level.
>
> 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 are implemented. A gap analysis can also provide a high-level overview of the controls in place that protect ePHI, without engaging in the comprehensive evaluation required by a risk analysis.[3]

Although HIPAA does not require specific types of risks assessments nor does it require the risk assessment to be documented in a certain manner, OCR's Guidance provides instructions to covered entities on what a thorough risk assessment should entail. A summary of the common elements that OCR wants analyzed in a risk assessment is as follows:[4]

1. Scope: The risk analysis should consider all ePHI received, maintained or transmitted as well as the source and location of the ePHI.

2. Data Collection: Entities should ensure that they are analyzing all places where ePHI is collected, stored or transmitted, including electronic devices and networks.

3. Threats and Vulnerabilities: All technical vulnerabilities as well as non-technical vulnerabilities should be identified. It is of note that OCR utilizes the definition of vulnerability found in NIST Special Publication 800-30 as "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in

a security breach or a violation of the system's security policy."

4. Security Measures: All current security measures, such as encryption, should be identified and assessed.

5. Threat Occurrences and Risk: The likelihood of threats and their impact should be identified as well as the risk level arising from such threat.

6. Documentation, Review and Updates: The risk analysis should be documented with enough detail to confirm it was accurate and thorough and should also be reviewed and updated regularly.

All covered entities as well as business associates should ensure that they are undertaking proper and thorough risk assessments, which should also be reviewed and updated regularly. In addition, the risk assessment is just one part of a broader HIPAA compliance program that covered entities should have in place to comply with HIPAA as well as other state and federal privacy regulations. If you have any questions regarding HIPAA compliance issues, please contact Stephanie T. Eckerle at seckerle@kdlegal.com, Stacy Walton Long at slong@kdlegal.com or your regular Krieg DeVault attorney.

[1] Risk Analyses vs. Gap Analyses – What is the Difference? (the "Guidance"), https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-april-2018.pdf.

[2] See 45 CFR § 164.308.

[3] Guidance, pg. 1.

[4] *See* Guidance, pgs. 1-2 for a detailed list of risk assessment contents.