E-BRIEF SERIES

Healthicity

Five Risk Analysis Essentials For HIPAA Compliance

WRITTEN BY STEVE SPEARMAN

Performing a risk analysis is the cornerstone of HIPAA compliance, therefore it's crucial to understand the regulations that require risk analysis, as well as how to conform to these rules in the best way possible. In this eBrief we will outline security risk analysis guidelines and essentials so that you can make informed decisions about your organization's risk analysis policies.

E-BRIEF SERIES

Healthicity

Five Risk Analysis Essentials For HIPAA Compliance

THE IMPORTANCE OF RISK ANALYSIS

Risk analysis is a methodical, proactive process of identifying risks to the confidentiality, integrity, and availability of an organization's electronic protected health information (ePHI). Providers who handle protected patient information must regularly review their systems to protect the security of delicate data.

Risk analysis allows providers to safeguard against vulnerabilities to prevent data breach or other dire security events. Using risk analysis best practices supports better security for patient health data, and is a key requirement of the HIPAA Security Management Process Standard and a major requirement for organizations seeking payment through the Medicare and Medicaid, Meaningful Use Program.

Following risk analysis best practices and guidelines will help your organization to remain HIPAA compliant, prevent data breach, and damage to your bottom line.

PERFORM AN ANNUAL RISK ASSESSMENT

HIPAA doesn't specify how often you should perform a risk analysis, but Meaningful Use does. Meaningful Use requires covered entities to either conduct a risk analysis or conduct a review of their most recent risk analysis every year during the reporting period.

Most information security experts would say that best practice is to conduct a risk analysis every year. This is true even if an organization is not involved with Meaningful Use. An organization should also do a risk analysis if it goes through a significant operational change, such as moving to a new building or adopting a new electronic health record.

We recommend that organizations adopt policies that require a full risk analysis at a minimum of every three years with reviews in the intervening years, unless there's a significant change in operations.

$4.8 MILLION VIOLATION

Providers found guilty of violating HIPAA standards face both financial devastation and reputational risk. A willful neglect violation that is not corrected can be anywhere from $10,000 to $50,000 for each violation. A prime example and one of the largest violations to date, occurred in 2014, when the New York Presbyterian Hospital and Columbia University were fined $4.8 million after the OCR investigated a HIPAA breach. A lack of technical safeguards for a network containing ePHIs resulted in patient records being easily accessible on Google.

COMPLETE YOUR RISK ASSESSMENT ON TIME

The deadline for conducting your 2016 Risk Analysis is December 31, 2016. Unfortunately, there's been a lot of confusion about this deadline. Initially, the rulemaking and guidance from the Office of the National Coordinator (ONC) made it clear that the risk analysis had to be conducted prior to the end of a covered entity's Meaningful Use reporting period. However, updated guidance from CMS from late 2014 indicated that the risk analysis can be done prior to attesting or during the calendar year of the reporting period, whichever comes first.

So based on the formula above, the risk assessment must be completed by December 31, 2016.

A FULL REVIEW VERSUS A FULL RISK ANALYSIS

A review is iterative. A review requires the assessor to document updates and changes that have occurred since the last risk analysis. This should include documenting security incidents, updates to policies, changes in IT asset inventory, and other operational changes. The review should then record working controls and recommend new controls and measures that should be considered to address current security issues.

THE DIFFERENCE BETWEEN A MEANINGFUL USE RISK

Analysis and a HIPAA Risk Analysis.

In the past, there was no difference between the two, however, the rulemaking beginning with Stage 2 and carried over to Stage 3 somewhat narrowed the scope of the risk analysis requirement for Meaningful Use purposes. Specifically, it would allow a covered entity to restrict the scope of its "Meaningful Use risk analysis" to its Electronic Health Record and supporting assets.

There may be cause for concern regarding the change because HIPAA requires entities to assess the risks associated with all their assets. For minimal extra effort, providers and hospitals can conduct a risk analysis that will meet the requirements of both HIPAA and Meaningful Use. This is what providers should do.

THE RELATIONSHIP BETWEEN THE HIPAA EVALUATION STANDARD AND RISK ANALYSIS

The relationship is simple. HIPAA's evaluation standard requires covered entities to understand and document the risks associated with operational decisions and changes. Risk analysis is the most important tool that entities have for evaluating those changes.

DEVELOP IN-HOUSE EXPERTISE OR HIRE AN EXPERT

A covered entity can conduct its own risk analysis. However, the risk analysis has to be thorough enough to pass an audit, and many covered entities and physicians don't have the resources, time, or expertise to conduct a risk analysis that would pass muster. If organizations wish to conduct their own risk analysis, they should commit to the resources needed to develop in-house expertise and to acquiring the tools needed to perform the risk analysis.

RISK ANALYSIS ACCEPTED STANDARDS

It is necessary to follow accepted standards and best practices related to conducting a risk

analysis. The most common reference is NIST Special Publication 800-30, a Guide for Conducting Risk Assessment.

Broadly speaking, a covered entity needs to identify the assets it uses to process, transmit, store, and manage ePHI. They should also categorize those assets according to risk and document the controls currently in place to protect those assets, controls that are absent, and those that need to be added in order to secure ePHI to a reasonable level.

COMMON PITFALLS TO AVOID

There are a number of common pitfalls that people should watch out for. For example, a person or a covered entity using nothing but a checklist to run a risk analysis may run into some trouble. Many risk analysis experts use checklists in our practices, but on their own, checklists cannot sufficiently identify risks to the degree that regulations require. For example, most checklists are regulation and policy-focused. So a checklist asking you to confirm the presence of a policy required by a regulation is useful for determining compliance risk. However, a checklist will not tell you whether an exploit exists on a particular machine that could jeopardize the security of ePHI.

Another common pitfall would be failing to perform an inventory. Any risk analysis method that does not include an IT asset inventory is likely flawed and insufficient. Covered entities need to identify and know the risks of the assets they use to store and transmit ePHI.

A security risk analysis burdens organizations with knowing the risks and threats to ePHI, not just checking off regulatory requirements and policies. A covered entity must have a risk analysis policy and procedure in place that will properly identify risks and threats to ePHI.

CONCLUSION: RISK ANALYSIS AND HIPAA COMPLIANCE

Performing a risk analysis is crucial for protecting your organization from fines, security breach, and HIPAA violation. Staying compliant doesn't have to be difficult though, compliance can be as simple as following basic guidelines such as:

- Conducting an annual risk assessment
- Knowing the difference between a Meaningful Use risk analysis and a HIPAA risk analysis
- Completing your risk analysis on time
- Avoiding common pitfalls such as using an overly general checklists