Codify
BY AAPC

Health Information Compliance Alert

HIPAA Compliance: When Disaster Strikes: Ask 4 Questions to Evaluate Breach Risk

Breach notification rules have changed are you up-to-speed?

You think you have a potential breach of protected health information (PHI). What now? First, don't panic instead, follow these four steps to evaluate the breach risk.

Important: The breach notification regulation under the HIPAA Omnibus Final Rule "actually replaces the 'harm threshold' requirement with the requirement to determine the 'risk of compromise,'" stated Lisa Gallagher, BSEE, CISM, CPHIMS, in a recent HIMSS Privacy and Security Committee blog posting. "This means that any impermissible use or disclosure of PHI is presumed to be a breach unless you're able to demonstrate, through a risk assessment, that there is low probability of compromise."

With an aim to make the assessment of a potential breach more objective (because "harm to an individual" is pretty subjective), the Omnibus Rule provides four specific factors to consider when you're performing the risk assessment for a possible breach, Gallagher pointed out.

Factor 1: What's the Extent & Nature of the PHI?

For the first risk factor, you need to "evaluate the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification," instructs Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, VT. Consider the following:

- The information's financial and clinical sensitivity;
- Whether direct or indirect identifiers are included;
- Whether the information can be linked for re-identification; and
- Whether the person receiving the PHI will have the ability to re-identify the PHI.

You need to analyze the types of PHI involved in the potential breach, instructed a recent health law update by **Quarles & Brady LLP (Q&B**). "Clearly, risk increases when a potential breach involves sensitive financial information, such as credit card numbers, social security numbers, or other information that increases the risk of identity theft."

"In addition, if clinical information is involved in a potential breach, covered entities [CEs] and business associates [BAs] should consider the nature of the services or other information (e.g., more sensitive information such as mental health or AODA information would increase risk), the amount of detailed clinical information exposed in the breach or, if the PHI involves only limited identifiers, whether the PHI can be re-identified based on context and other available information," Q&B stated.

Factor 2: Who Received the PHI?

The identity of the person or persons who accessed or received the PHI is also paramount to your evaluation of breach risk. Sheldon-Dean advises that you consider:

- Is the identity of the unauthorized person known?
- Does the person have obligations to protect the privacy and security of PHI?
- What is the likelihood that the information would be used by an unauthorized recipient to adversely affect individuals or for personal gain?

What this means: If the recipient is another entity bound by HIPAA Privacy and Security Rules, the risk is lower, Q&B explained. "On the other hand, if the PHI is used by or disclosed to a wrongdoer ... it's more likely that the use or disclosure would constitute a breach."

Factor 3: Was the PHI Viewed?

Whether the PHI was actually acquired or viewed is another key factor you need to evaluate. According to Sheldon-Dean, you must consider:

Was there opportunity to acquire or view the PHI?

Was the potential breach discovered and prevented before the PHI was viewed or acquired?

What information are you relying on?

"Like the others, this factor is simply repackaged from the previous version of the breach notification rule," Q&B noted. You "must determine whether the PHI was actually acquired or viewed, or whether there was only opportunity for the information to be acquired or viewed."

"For instance, if a laptop is lost or stolen and later recovered, and a forensic analysis shows that the PHI on it was never accessed, it is less likely that a breach has occurred," Q&B said.

Factor 4: Was the Risk Mitigated?

"Evaluate the extent to which the risk to the PHI has been mitigated," Sheldon-Dean states. How quickly did you react to the potential breach? What steps did you take to ensure that the PHI remained safe from wrongful use? Consider:

- Were satisfactory assurances obtained that the PHI will not be further used or disclosed?
- The person providing satisfactory assurances.
- Are the satisfactory assurances in writing?

Crucial: "By quickly mitigating any risk to PHI that was improperly used or disclosed, [CEs and BAs] may lower the risk that the use or disclosure will constitute a breach," Q&B stated. "For example, the [CE] may mitigate risk by having a recipient of impermissibly disclosed PHI provide assurances (e.g., a confidentiality agreement) that the PHI will be destroyed or will not be further used or disclosed."