How To Analyze A HIPAA Breach

Insights
2.03.14

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) and subsequent regulations have changed several aspects of compliance with HIPAA, including the way covered entities should think about misuses of Protected Health Information (PHI).

When a misuse of PHI occurs, HIPAA requires covered entities to conduct a thorough, good-faith analysis to determine whether the misuse rises to the level of a breach. A "breach" is the unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of such information.

Depending on the severity of the breach, covered entities could face reporting and notification requirements that include notifying the Department of Health and Human Services (HHS), affected individuals, and even the media. For this reason, whether a misuse rises to the level of a breach requires careful examination. In brief, a breach contains the following elements: 1) an unauthorized acquisition, access, use, or disclosure; 2) of unsecured PHI; 3) resulting in an impermissible disclosure under the privacy rule; 4) that compromises the security or privacy of such PHI; and 5) to which an exception does not apply.

Under the final regulations issued by HHS, which became effective on September 23, 2013, the concept of what "compromises" the security or privacy of PHI has changed. Previously, a breach occurred only if there was a significant risk of financial, reputational, or other harm to the individual. But the 2013 final regulations remove this "harm standard" and instead require a four-part risk assessment intended to focus on the risk that PHI has been compromised in a more objective way.

The 2013 regulations provide that a covered entity must presume that an acquisition, access, use, or disclosure of PHI in violation of the privacy rule is a breach. This presumption holds unless the covered entity demonstrates that there is a "low probability" that the PHI has been compromised based on a risk assessment which considers at least the following factors: 1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification, 2) the unauthorized person who used the PHI or to whom the disclosure was made, 3) whether the PHI was actually acquired or viewed, and 4) the extent to which the risk to the PHI has been mitigated.

Here's a closer look at how these are defined:

The nature and extent of the PHI involved

Based on HHS guidance, covered entities should consider whether the disclosure involved PHI that is of a sensitive nature, including the types of identifiers and the likelihood of re-identification. Social security numbers would be considered sensitive items, whereas a city or state identifier would not be as sensitive. Entities should consider the likelihood that someone could suffer financial or reputational harm based on the information to determine its level of sensitivity.

The unauthorized person who used, accessed, or received the PHI

Consider whether the unauthorized person is trained in HIPAA compliance, has obligations to protect the privacy and security of the information, has a track record of protecting similar information, and can be obligated to return it. HHS emphasizes that this factor should be considered in combination with the first factor regarding the risk of re-identification.

Whether the PHI was actually acquired or viewed

Analyze whether the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed. Entities may have the technology to confirm that information was unviewed, or they may be able to lock a lost cell phone or destroy files remotely in order to protect themselves under this factor.

The extent to which the risk to the PHI has been mitigated

Finally, covered entities must evaluate the extent to which the risk to the PHI has been mitigated. If the PHI is no longer in the entity's possession, consider factors such as how easily it can be duplicated.

For more information, contact the author at TGeorge@fisherphillips.com or 504.522.3303.