When to Send a Breach Notification: New HIPAA Rules Revise “Harm” Standard

By Diana Warner, MS, RHIA, CHPS, FAHIMA

The HITECH Act’s omnibus HIPAA modification final rule, released January 25, 2013, finalized sweeping changes to privacy and security regulations. Though much of the proposed rule was adopted, the omnibus rule included major changes made to the “harm threshold” standard included in the breach notification interim final rule. The harm standard as proposed would have required notice of a breach of privacy or security to the affected individual if the breach posed significant risk of financial, reputational, or other harm to that individual. The original intent was to prevent individuals from being inundated with “inconsequential” breach notifications and to minimize the potential for apathy if breach after breach were reported.

The Office for Civil Rights (OCR) received numerous concerns that the risk of harm as outlined in the interim final rule was too subjective. OCR revised this standard and outlined a more objective way to measure when a breach creates a situation of “significant risk” and notification is warranted. The standard outlines factors to be considered when assessing whether to report a breach. The final rule was effective March 26, 2013. Organizations may begin to use the new subjective standard now or continue to use the old harm standard until the compliance date of September 23, 2013-at which point the new standard must be applied. At minimum, organizations should begin developing their risk assessment to capture the new subjective standards in order to be ready by the compliance date.

Is It a Breach?

The HITECH-HIPAA final rule includes an automatic presumption that any impermissible use or disclosure of protected health information (PHI) constitutes a breach. This implies that notification is necessary in every situation except when a covered entity or business associate determines that there is a low probability the PHI has been compromised, as defined in the rule. There are exceptions to the definition of a breach, including:

- Unintentional acquisition by a workforce member
- Inadvertent disclosures from an authorized person to another authorized person
- Disclosures where there is a good faith belief that the information could not be reasonably retained

The final rule removes the exception to the breach definition related to limited data sets that do not include birthdates or ZIP codes. Now, following an impermissible use or disclosure of any limited data set, covered entities and business associates must either notify the individuals or perform a risk assessment and determine if breach notification is needed.

When to Report

Covered entities must notify the Department of Health and Human Services (HHS) of breaches of unsecured PHI affecting 500 or more individuals as well as the affected individuals within 60 days. For breaches affecting fewer than 500 individuals, the final rule clarified that covered entities must notify HHS within 60 days after the end of the calendar year in which the breaches were discovered, instead of when the breaches occurred.

Creating a Risk Assessment

The HITECH-HIPAA final rule defines a breach as an impermissible “acquisition, access, use, or disclosure” of PHI. Since there is a presumption that a breach has occurred following every impermissible use or disclosure, entities may decide to notify individuals without performing the risk assessment. However, the decision to complete a risk assessment is left up to the organization. The final rule calls for covered entities, as well as business associates and their subcontractors, to use a risk

assessment to determine if a suspected breach did occur and to gauge the probability that the PHI has been compromised. There are a minimum of four key factors that now need to be considered in assessing whether breaches should be reported:

- Whether the information included patient identifiers
- Who may have had unauthorized access to exposed data
- How likely it is the data was inappropriately viewed
- Whether the risk involved was quickly mitigated

OCR noted that, depending on the situation, other factors may need to be taken into consideration during the risk assessment. Organizations will need to change their approach for assessing the risk. Instead of trying to determine if the lost, unsecured PHI could cause financial or reputational harm to the individual, they will need to determine the likelihood that the information could be accessed or if it was found in a timely manner. The covered entity or business associate must consider all factors, and assessments are to be completed in good faith. If the assessment fails to demonstrate that there is a low probability that the PHI has been compromised, then breach notification is required.

Compromised PHI Examples

The following examples were included in the final rule to demonstrate situations where a risk assessment should be used in order to determine the existence of a "low probability" of a breach occurring. HHS states that it will issue additional guidance in the future to aid HIPAA-covered entities and business associates in performing risk assessments.

- A covered entity that inadvertently discloses a list of patient names, addresses, and hospital identification numbers. A risk assessment would likely determine high probability that the PHI has been compromised.
- A covered entity that inadvertently disclosed a list of patient discharge dates and diagnoses would need to consider whether any of the individuals could be identified based on the diagnosis and the size of the community served by the covered entity. In a large community, the risk assessment may show that identification of the individuals is a low probability and would not require a breach notification. In a small community, however, the possibility of identifying the individuals may be higher, thereby failing the low probability assessment and requiring a breach notification.
- In a case involving a lost or stolen laptop that has been recovered, if forensic analysis shows that the PHI on the computer was not accessed then the covered entity or business associate could determine that the information was not compromised.
- If a covered entity mailed information to the wrong individual who opened and reviewed the information, then called the covered entity to let them know the information was mailed to the wrong person, there would be a high probability that the information was compromised and a breach notification would be required.

The best approach to minimize, and avoid altogether, the need for determining the probability of a breach is to secure paper records and encrypt all data.

References

Department of Health and Human Services. "Other Requirements Relating to Uses and Disclosures of Protected Health Information." *Federal Register*. 45 CFR parts 160 and 164. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

McGee, Marianne Kolbasuk. "HHS Omnibus: Impact on Breach Notices." *Healthcare Info Security*. January 21, 2013. http://www.healthcareinfosecurity.com/hipaa-omnibus-impact-on-breach-notices-a-5436.

Williams, Rebecca et al. "New Omnibus Rule Released: HIPAA Puts on More Weight." Davis Wright Tremaine LLP website. January 23, 2013. http://www.dwt.com/New-Omnibus-Rule-Released-HIPAA-Puts-on-More-Weight-01-23-2013/.

Diana Warner (diana.warner@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
Warner, Diana. "When to Send a Breach Notification: New HIPAA Rules Revise “Harm” Standard" *Journal of AHIMA* 84, no.4 (April 2013): 42-43.