Breach Notification Triggers Receive Update

Save to myBoK

By Rita Bowen

The HIPAA Omnibus Rule, the new Final Rule modifying HIPAA, was published in the *Federal Register* on January 25, 2013. The amended rule went into effect on March 26 and full compliance is expected by September 23. For HIM professionals, the most far-reaching of the changes to HIPAA is that business associates (BAs) will now assume their fair share of the responsibility for keeping data safe and secure. There is also financial incentive for BAs to comply.

After March 26, when breaches occur for which they are responsible, BAs must pay the cost of breach remediation. Beyond the financial implications, BAs will also be required to assess risk when a breach occurs and report breaches utilizing the same criteria as covered entities (CEs). BA agreements must all be updated, subcontractors of BAs must also have agreements, and BA breaches must be reported within 60 days.

The incorporation of BAs into direct HIPAA compliance to assess risk and report breaches drove the Department of Health and Human Services (HHS) to more clearly define a breach, to identify cases that are "not" a breach, and to establish rules surrounding its reporting. The update to the rule also provides four factors to determine if a breach has occurred.

Under the HIPAA Omnibus Final Rule, risk assessments focus more objectively on the risk that PHI has been compromised—versus a subjective valuation of "harm to an individual" resulting from a breach. The rule includes four criteria and 19 unique identifiers—categories of personal information potentially collected in the course of patient care—that could, in the event of a breach, link an individual to the care provided. This article explains both.

Risk Assessments: Four Factors to Consider

There are now four specific factors that CEs and BAs must consider when a breach occurs to adequately determine if PHI has been compromised and to what level reporting of that breach must be made.

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the protected health information or to whom the disclosure was made
- Whether the protected health information was actually acquired or viewed
- The extent to which the risk to the protected health information has been mitigated; for example, was the breached information received via facsimile and then destroyed or actually used and/or shared?

In a January 25, 2013 analysis of the modification to the HIPAA privacy, enforcement, and breach notification rules, AHIMA further explains each of these factors. At a minimum, CEs and BAs must assess risk using the four factors (found on page 26 of AHIMA's Analysis) listed above. Furthermore, the 19 unique identifiers page must be collected and included in each risk assessment.

19 Unique Identifiers to Include

In the past when organizations reported the occurrence of a breach, they were not required to include which identifiers were associated with it. Though it was done on particular risk assessments (CEs might have looked to see if certain social security numbers or medical record numbers were involved), it simply was not standard practice.

Now, per the new rule, unique identifiers must be included within each risk assessment. These identifiers are consistent with the original HIPAA rule and include:

- Name
- All geographic subdivisions smaller than a state (street address, city, county, precinct) (Note: ZIP code must be removed, but can retain first 3 digits if the geographic unit to which the zip code applies contains more than 20,000 people)
- For dates directly related to the individual, all elements of dates, except year (i.e., date of birth, admission date, discharge date, date of death)
- All ages over 89 or dates indicating such an age
- Telephone number
- Fax number
- Email address
- Social Security number
- Medical Record number
- Health Plan number
- Account numbers
- Certificate or license numbers
- Vehicle identification/serial numbers, including license plate numbers
- Device identification/serial numbers
- Universal Resource Locators (URLs)
- Internet Protocol addresses (IP addresses)
- Biometric Identifiers
- Full face photographs and comparable images
- Any other unique identifying number, characteristic, or code

While collecting and reporting each of these 19 unique identifiers for every potentially breached record seems tedious at best—and superfluous at worst—HHS has provided clear and thorough parameters for assessing risk and reporting breaches.

Impact on HIM

Both CEs and BAs must consider these more objective factors when conducting risk assessments to determine if the protected health information has been compromised and breach notification is necessary. The onus is on HIM professionals to educate staff and implement a breach risk assessment and reporting plan that incorporates all the HIPAA guidelines, including the four factors and 19 unique identifiers. In the wake of the new HIPAA rule, BAs and CEs must be proactive in their efforts to comply. As always, ongoing education, vigilance, and data governance are keys to success.

Rita Bowen, MA, RHIA, CHPS, SSGB is senior vice president of HIM and privacy officer and HealthPort.

Original source:
Bowen, Rita K.. "Breach Notification Triggers Receive Update" (Journal of AHIMA website), April 2013.
