Navigating a Compliant Breach Management Process

Save to myBoK

The purpose of AHIMA's new Breach Management Toolkit is to provide a comprehensive collection of resources and best practices to help healthcare organizations and health information management (HIM) professionals navigate their way through the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule and the overall breach management process. The toolkit is intended to raise awareness of the importance and responsibility of everyone within the organization to report HIPAA breaches to the appropriate designated personnel, as well as provide breach prevention education and training.

The HITECH-HIPAA Omnibus Final Rule modifies and clarifies the definition of a breach and risk assessment. From the first report of a potential breach through the final breach notification, many factors must be considered and accounted for, such as investigation, assessment, mitigation, education and training, state laws, response times, required notifications, and annual reporting of a breach to the Department of Health and Human Services (HHS), to name a few. Policies and procedures, a breach risk assessment, and other tools and guidance must be in place to ensure that the overall management of a breach is compliant with the HIPAA Breach Notification Rule.

The Current Breach Landscape

Since the enactment of the breach notification rule, breaches of all sizes involving various types of protected health information (PHI) have affected the healthcare industry. At the end of 2013, almost 28 million individuals in the US were impacted by a breach. The top three causes of a breach that compromised PHI included theft, unauthorized access/disclosure, and computer hacking.[1]

In addition to the affected patients, the impact and consequences of a breach extend to those involved in the inappropriate access as well as the reputation of the provider organization. The impact of diminished trust in an organization cannot be calculated in numbers. The financial expense, however, is more readily apparent. According to the 2014 Ponemon Institute's Fourth Annual Benchmark Study on Patient Privacy and Data Security, the economic impact of one or more data breaches for healthcare organizations in this study ranged from less than $10,000 to more than $1 million over a two year period. Based on the ranges reported by respondents, it was calculated that the average economic impact of data breaches over the past two years for the healthcare organizations represented in the study was $2 million. The study also found that theft and loss comprise the primary causes for breaches.[2]

Determining Between Incident, Violation, or Breach

Breaches exist in multiple forms and can occur in the smallest and largest of organizations. The media often uses the terms violation, incident, and breach interchangeably when reporting upon compromised PHI. Each of these phrases, however, has its own distinct meaning.

Defining an Incident

An incident is an event reported to the designated privacy and/or security official that will result in an investigation to determine the possibility of an impermissible use or disclosure of PHI. Upon completion of an investigation, an incident will be determined to be a violation or a breach in which appropriate actions will be taken, including sanctions to resolve any issues and meet compliance with all breach notification or organizational policy requirements (where applicable).

Defining a Violation

A violation of the HIPAA Privacy or Security Rule occurs in instances where unsecured PHI was acquired, used, or disclosed in a manner not permitted by the rule. Under the HITECH-HIPAA Omnibus Final Rule, published on January 25, 2013, an entity is required to presume the violation to be a breach unless one of three exceptions apply—the information can be rendered as unusable, unreadable, or indecipherable—or a completed risk assessment demonstrates low probability that the

PHI has been compromised. PHI that cannot be rendered as unusable, unreadable, or indecipherable to unauthorized persons through either encryption or destruction is considered to be unsecured.

Defining a Breach

The HITECH-HIPAA Omnibus Final Rule included final modifications to the Breach Notification Rule that replaced the interim final rule originally published in 2009. The term "breach" is now defined in 45 CFR 164.402. as "the acquisition, access, use, or disclosure of protected health information in a manner [not permitted by the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information." An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity (CE) or business associate (BA), as applicable, demonstrates—based on a risk assessment—that there is a low probability the PHI has been compromised. As a result, breach notification is necessary in all situations except those in which the CE or BA, as applicable, demonstrates there is a low probability that the PHI has been compromised.

The rule acknowledges that there are several situations in which unauthorized acquisition, access, use, or disclosure of PHI is so inconsequential that it does not warrant notification. Section 164.402 of the final rule identifies these exceptions as:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or other person acting under the authority of a CE or BA, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rule
2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA or organized healthcare arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule
3. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information[3]

To ensure this provision is applied uniformly and objectively by CEs and BAs, the final rule removed the harm standard and modified the risk assessment to focus on the probability that the PHI has been compromised, using a combination of factors identified in the rule that are more objective than the previous harm threshold standard.[4]

The final rule identifies four factors that make up a breach risk assessment, and requires individuals to include, at a minimum:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

A CE's or BA's analysis of the probability that PHI has been compromised following an impermissible use or disclosure must address each factor included above.

Other factors may also be considered when necessary. CEs and BAs must then evaluate the overall probability that the PHI has been compromised by considering all factors in combination.

Elements of the Breach Investigation Process

The organization should develop an organization-wide general policy and plan for conducting internal investigations. The investigation policy will address specific steps that should be followed when conducting an internal investigation. Some guidelines to consider include:

- Establish a breach response team
- Investigate each incident swiftly and completely
- Develop corrective action steps such as determining appropriate workforce sanctions
- Conduct periodic review of potential problem processes
- Fully follow through with any required legal obligations

Organizing a Breach Response Team

Composition of the breach response team will vary depending on the size of the organization. Ideally this will be a cross-functional leadership team whose members have a keen understanding of HIPAA privacy and security and are advocates for patients' right to privacy. In many cases, legal counsel may be determined to be the appropriate breach response team leader, and in other cases the compliance or privacy officer may be best fit for this role. In general some incidents may be straightforward and easily resolved. However in the case of willful intent or if complex cases include fraud and abuse violations, legal counsel involvement may be advisable. Selection of the members of the investigative response team will be determined by policy and additional members may be appointed based on the extent of the potential violation.

Conducting the Investigation

The breach investigation process is a systematic approach to making a definitive determination as to whether a breach has taken place. Conducting internal investigations effectively is one of the most important steps to establish a potential violation of the law. An organized series of steps that can be followed during an investigation will help provide consistency, objectivity and avoid leaving out any key procedures. The administrative requirements of HIPAA Privacy Rule 164.530 provide the framework for a thorough investigation by requiring covered entities to provide a process for individuals to make complaints and then requiring documentation of those complaints and their disposition—essentially requiring an investigation.

Mitigating Harmful Effects of a Breach

When an impermissible access, use, or disclosure is substantiated, mitigation is required. The HIPAA Privacy Rule mitigation standard states that a covered entity must mitigate, to the extent practicable, any harmful effect that is known to the CE of a use or disclosure of PHI in violation of its policies and procedures or the requirements of the rule. Additionally, under the breach notification rules, mitigation is one of the factors that must be evaluated in determining whether the PHI has a low probability of compromise.

Mitigation of breach incidents typically requires a series of actions or processes that will assist in the identification of root causes of the breach to help organizations understand how the incident happened and prevent future occurrences. Every mitigation process is likely to include an investigatory review of current privacy and security protocols involved in the incident.

Performing a Risk Assessment

Within the scope of the breach investigation overview, it is essential to conduct the required incident risk assessment for every identified incident where PHI is involved unless the organization decides to move ahead with notification without trying to demonstrate low probability. To establish whether or not PHI has been compromised, the following four factors must always be documented:

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

Breach Determination and Risk Assessments

Every reported privacy and/or security incident warrants immediate attention and a full investigation to determine whether the incident is just a violation, or if in fact it is a breach by definition under the HITECH-HIPAA Omnibus Rule. It is critical that the determination is made accurately and in a timely manner so the appropriate actions can be taken—such as applying sanctions or following breach notification requirements. Covered entities have 60 days from the date of discovery to ensure compliance with all breach notification requirements.

A reported incident can be a violation, a breach, or neither. As discussed in Section III of the final rule, the process and investigation for determining a breach must be highly detailed, thorough, accurate, and completely documented. It must capture all elements of the incident such as date, type of PHI involved, details of what happened, and person(s) involved—including both the person who inappropriately accessed as well as the individual whose PHI was inappropriately accessed or disclosed.

Required Breach Reporting for CEs and BAs

CEs and BAs are required to notify HHS of any breach of unsecured PHI affecting 500 or more individuals without unreasonable delay and in no case later than 60 days from the discovery of the breach. This notification must be submitted electronically. In the event that a breach impacts more than 500 individuals across multiple states, only one HHS report should be submitted, though there may be multiple media notifications. The rule clarified that some breaches involving more than 500 individuals who are residents in multiple states may not require notice to the media, provided no one jurisdiction included more than 500 affected individuals.

For any breach affecting fewer than 500 individuals, CEs and BAs are required to notify HHS annually. All notifications occurring within a calendar year must be submitted within 60 days of the end of the calendar year in which the breach was discovered.

Breach Management Toolkit Available

AHIMA's Breach Management Toolkit provides sample forms, policies and procedures, and workflow diagrams as well as a breach risk assessment template to assist with the determination and necessary steps to stay in compliance with federal law. The toolkit is free to AHIMA members, and is available online [...].

Notes

1. Melamedia. "HIPAA & Breach Enforcement Statistics for April 2014." http://www.melamedia.com/HIPAA.Stats.home.html.
2. The Ponemon Institute. "Fourth Annual Benchmark Study on Patient Privacy and Data Security." March 12, 2014. http://www2.idexpertscorp.com/ponemon-report-on-patient-privacy-data-security-incidents/.
3. Department of Health and Human Services. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 78, no. 17 (January 25, 2013). http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.
4. AHIMA. "Performing a Breach Risk Assessment." *Journal of AHIMA* 84, no. 9 (Sept 2013): 66-70.

References

AHIMA. Breach Management Toolkit: A Comprehensive Guide for Compliance. Chicago, IL: AHIMA Press, April 2014.

Department of Health and Human Services Office for Civil Rights. "HIPAA Administrative Simplification Regulation Text 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013)." March 2013. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.

Prepared by

Katherine Downing, MA, RHIA, CHPS, PMP

Article citation:
Downing, Katherine. "Navigating a Compliant Breach Management Process" *Journal of AHIMA* 85, no.6 (June 2014): 56-58.