Navigating a Compliant Breach Management Process (2018 Update)

Save to myBoK

This Practice Brief supersedes the June 2014 Practice Brief "Navigating a Compliant Breach Management Process."

The Health Insurance Portability and Accountability Act (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, including:

- Investigation
- Assessment
- Mitigation
- Education and training
- State laws
- Response times
- Required notifications
- Annual reporting of a breach to the Department of Health and Human Services (HHS)

Policies and procedures, a breach risk assessment, and other tools and guidance must be in place to ensure the overall management of a breach is compliant with the HIPAA Breach Notification Rule.

The purpose of AHIMA's updated 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 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 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. By the middle of 2017, nearly 175 million individuals in the US have been impacted by a breach.[1] The top three causes of a breach that compromised protected health information (PHI) included theft, hacking/IT incident, and unauthorized access/disclosure.[2]

In addition to the affected patients, the impact and consequences of a breach extend to those involved in the inappropriate access as well as an entire provider organization, who can have their reputation harmed. The impact of diminished trust in an organization cannot be calculated in numbers. The financial expense, however, is more readily apparent. According to the 2016 Ponemon Institute's Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, it is estimated that data breaches could be costing the healthcare industry $6.2 billion over the two-year span of their most recent study. The cost of a breach over a two-year period is estimated to be more than $2.2 million per breach. The study also confirms criminal attacks are the leading cause of data breaches in healthcare.[3]

Ransomware is more prevalent than ever. There have been over 4,000 daily ransomware attacks since early 2016. Just as with any other type of breach, both covered entities (CEs) and business associates (BAs) need to follow HIPAA to prevent and recover from a ransomware attack.[4]

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 about 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 investigation completion, an incident can 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

A breach is 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 CE or 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.

Criminal attacks are a leading cause of data breaches in healthcare and it is important to note that HHS published guidance on ransomware describing under what circumstances a ransomware attack would be considered a breach. The guidance stated that when electronic protected health information (ePHI) is encrypted as a result of a ransomware attack, a breach has occurred. The ePHI that is encrypted by the ransomware is assumed to have been acquired since there is unauthorized possession or control of the information. Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the Breach Notification Rule, a breach of the ePHI is presumed to have occurred. The guidance goes on to describe that organizations would then continue to follow breach management processes and rules in evaluating the probability that the PHI has been compromised.4

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.[5]

To ensure CEs and BAs uniformly and objectively apply this provision, 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.[6]

The 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.

Following the HIPAA security measures can help prevent ransomware attacks, which are on the rise. HIPAA outlines the following security measures to reduce the risk of an attack:

- Implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to ePHI and implementing security measures to mitigate or remediate those identified risks.
- Implementing procedures to guard against and detect malicious software.
- Training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections.
- Implementing access controls to limit access to ePHI to only the persons or software programs requiring access.[7]

Another resource to mitigate ransomware attacks is the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. This crosswalk can be used to compare the CE's or BA's security program and identify and address potential gaps, thereby strengthening the program.

Elements of the Breach Investigation Process

An 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, it may be determined that legal counsel is the appropriate breach response team leader, and in other cases the compliance or privacy officer may be the best fit for this role. In general, some incidents may be straightforward and easily resolved. In the case of willful intent or if complex cases include fraud and abuse violations, however, 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 and objectivity, as well as 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 require 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.

An organization may consider mitigation steps to lessen the negative impact of the impermissible access, use, or disclosure. Re-secure the PHI and obtain strong assurances that the information will not be further used or disclosed.

Healthcare entities should:

- Take action quickly—this may lessen the risk to the PHI
- Mitigation for impermissible disclosures should include:
    - Attempts to recover or ensure the recipient has destroyed the PHI
    - Written confirmation of destruction
- Mitigation for impermissible access, use, or disclosure should include:
    - Assurances from the recipient that the PHI will not be further used or disclosed
    - Written assurances, such as through a confidentiality agreement
- Technical procedures such as the ability to wipe devices for incidents involving ePHI

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 and business associates 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 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 the PHI as well as the individual whose PHI was inappropriately accessed or disclosed.

The AHIMA Breach Management Toolkit explains that determining the low probability of compromise may be done through a completed risk assessment to assist in determining the extent of the potential threat and the risk associated with it. Taking the four factors described above into consideration, the probability can be scored by evaluating the likelihood and potential impact that the information has been compromised.

Adapting the National Institute of Standards and Technology's (NIST's) Security Risk Analysis Tool, the following is one example of how an organization might choose to evaluate the low probability of compromise. The likelihood that the PHI has been compromised can be described as high, medium, or low and defined as follows:

- High: The information more than likely could be impermissibly used or disclosed
- Medium: The information may be impermissibly used or disclosed
- Low: The information has a minimal, rare, or seldom probability of being impermissibly used or disclosed

The impact of the impermissible use and disclosure can be described as severe, moderate, or minimal and defined as:

- Severe: The PHI in question easily identifies the patient and could be impermissibly used or disclosed.
- Moderate: The PHI in question has the potential of identifying the patient and the probability of improper use or disclosure is uncertain.
- Minimal: The PHI in question may or may not identify the patient; however, satisfactory assurances have been obtained that the information will not be impermissibly used or disclosed.[8]

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 available in the AHIMA store at https://my.ahima.org/search/toolkits. A new toolkit update is coming in 2018.

Notes

1. Ziskovsky, Tracy. "2017 HIPAA Breach Stats: Where Are We At?" HIPAA ONE blog. August 3, 2017. www.hipaaone.com/2017-hipaa-breach-stats/.
2. Melamedia, LLC. "Scores of Entities Forced to Make HIPAA Changes Due to Patient Complaints." 2017. www.melamedia.com/category_s/102.htm.
3. Ponemon Institute. "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data." May 2016. www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf.
4. Department of Health and Human Services. "Fact Sheet: Ransomware and HIPAA." www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es.
5. Ibid.
6. 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). www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.
7. Department of Health and Human Services. "Fact Sheet: Ransomware and HIPAA."
8. AHIMA. *Breach Management Toolkit: A Comprehensive Guide for Compliance (Draft).* Chicago, IL: AHIMA Press, in press.

References

AHIMA. *Breach Management Toolkit: A Comprehensive Guide for Compliance.* Chicago, IL: AHIMA Press, April 2014. https://my.ahima.org/store/product?id=61479.

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. www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.

Department of Health and Human Services Office for Civil Rights and National Institute for Standards and Technology. "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework." www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

Prepared By

Diana Warner, MS, RHIA, CHPS, CPHI, FAHIMA

Prepared By (Original)

Katherine Downing, MA, RHIA, CHPS, PMP

Download
Breach Management Toolkit Available Online

https://my.ahima.org/search/toolkits

AHIMA's Breach Management Toolkit, free to AHIMA members, includes several tools to aid with breach risk assessment. These include a sample tool that may be utilized to assist in scoring each factor and documenting the risk assessment; a sample case to help demonstrate low probability of compromise; and a decision tree diagram that follows the workflow from the point an incident is reported through the actions necessary for compliance. A new toolkit update is coming in 2018.