AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION

Breach Management TOOLKIT

A Comprehensive Guide for Compliance

AHIMA
American Health Information Management Association®

Breach Management TOOLKIT

ISBN: 978-1-58426-674-7
AHIMA Product No.: ONB202618
AHIMA Staff:
Chelsea Brotherton, *Assistant Editor*
Anne Zender, *Senior Director, Periodicals*

For more information about AHIMA Press publications, including updates, visit ahima.org/education/press

American Health Information Management Association
233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601

AHIMA.ORG

1102.18

TABLE OF CONTENTS

FOREWORD

On August 24, 2009, the US ***Department of Health and Human Services (HHS)*** published 45 CFR Parts 160 and 164, Breach Notification for ***Unsecured Protected Health Information***; Interim Final Rule, to implement the breach notification provisions of the ***Health Information Technology for Economic and Clinical Health (HITECH) Act*** of 2009. The HITECH Act requires HIPAA-covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured ***protected health information (PHI)***.[1] The interim final rule included a risk assessment approach to determine if there was a significant risk of harm to the individual as a result of the impermissible use or disclosure—the presence of which would trigger breach notification.

On January 25, 2013, ***HHS*** published modifications to the ***Health Insurance Portability and Accountability Act (HIPAA)*** Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act (GINA); Other Modifications to the HIPAA Rules (also referred to as the Omnibus Final Rule). This encompasses significant modifications for breach notification, of which breach investigation, risk assessment, risk mitigation, and reporting remain essential components.

This toolkit is intended to provide guidance on the overall management of a breach.

Disclaimer: For the purposes of this toolkit, federal guidelines are discussed, but state laws must always be reviewed to determine full compliance needs.

The following resources can be used to identify some state specific requirements;

- The National Conference of State Legislatures: http://www.ncsl.org/research/health/hipaa-a-state-related-overview.aspx
- The National Institutes of Health: http://privacyruleandresearch.nih.gov/pr_05.asp

Note: Boldface italicized *terms throughout the toolkit indicate those items defined in the glossary (See Appendix A).*

AUTHORS

Margaret (Peg) Schmidt, RHIA, CHPS
Barb Beckett, RHIT, CHPS
Dana DeMasters, MN, RN, CHPS
Wes Morris, CHPS, CIPM, HCISPP
John Young, III, RHIA, CHPS, CPHIMS
Diana Warner, MS, RHIA, CHPS FAHIMA

ORIGINAL AUTHORS

Sheena Albright, RHIT
Jennifer Bourn, RHIT
Robin Bowe, BSN, RN, CHC
Rita Bowen, MA, RHIA, CHPS, SSGB
Rebecca A. Buegel, RHIA, CHPS, CDIP, CHC
Angie Fergen, RHIA, CHPS
Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA
Susan M. Lucci, RHIT, CHPS, CMT, AHDI-F
Katherine Maddox, RHIA, CHC
Phyllis Maher, RHIA
Kara Martin, RHIA
Debra Mikels, OTR/L
Mary Poulson, MA, RHIT, CHC, CHPC
Rebecca Reynolds, EdD, RHIA, FAHIMA
Harry Rhodes, MBA, RHIA, CHPS, CDIP, CPHIMS, FAHIMA
Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA
Margaret (Peg) Schmidt, RHIA, CHPS
LaVonne Wieland, RHIA, CHP

ACKNOWLEDGEMENTS

Nancy Davis, MS, RHIA CHPS
Kathy Downing, MA, RHIA, CHPS, PMP
Rose T. Dunn, MBA, RHIA, CPA, FACHE
Kathy J. Edlund, M.M, RHIA
Elisa R. Gorton, MAHSM, RHIA, CHPS
Rose Marie Grave, RHIT, CPEHR, RAC-CT
Aviva Halpert, MA, RHIA, CHPS
Lesley Kadlec, MA, RHIA
Stephanie Luthi-Terry, MA, RHIA, CHPS, FAHIMA
Marcia Matthias, MJ, RHIA, CHPC
Kelly McLendon, RHIA, CHPS
Sue Nathe, RHIT
Kristen A. Piccirillo, RHIA, CCS, NASM-CPT
Laurie Peters, RHIA, CCS
Theresa Rihanek, MHA, RHIA, CCS
Colleen Simianer, RHIA, CHP, CCS
Margie Stackhouse, RHIA, CPC
Jami Woebkenberg, MHIM, RHIA, CPHI

INTRODUCTION

From the first report of a potential breach through the final breach notification, many factors must be considered and accounted for. These include but are not limited to investigation, assessment, **mitigation**, education and training, state laws, response times, required notifications, and annual reporting of a breach to the HHS. Additionally, 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 purpose of this 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. It is to be used as a framework and reference guide to assist with the breach investigation, determination, mitigation, notification, reporting processes, and to provide assistance with understanding and complying with federal regulations within the required time frame required by federal law. It is intended to bring awareness of the importance and responsibility of training work force members in breach notification, identification, and prevention.

Sample forms, policy and procedures, and workflow diagrams, including a breach risk assessment template, are provided to assist with the determination and next steps necessary to stay in compliance with federal law. Please note that the information contained in this toolkit does not address individual state statutes that may, at times, compete with HIPAA federal rules and guidelines.

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. It seems as if every day the media features one story or another about a breach of PHI. An analysis of reported breaches from the HHS Office of Civil Rights identified that in the first half of 2017, almost 175 million individuals were impacted by breaches from 1,996 organizations.[2] Business associates were involved in approximately 409 breaches with approximately 31 million individuals potentially exposed. The top three causes of PHI data breaches were theft, hacking/IT incident, and unauthorized access/disclosure.[3]

The consequences of a breach stretch far beyond the patients directly affected; those involved in the impermissible access and/or disclosure are also impacted. The major fallout from a data breach is an organization's reputation, which is likely to be hurt by the diminished trust factor of the overall organization—a cost that cannot be calculated in numbers. However, the financial expense can be just as damaging. According to the 2016 Ponemon Annual Benchmark Study on Patient Privacy and Data Security, it is estimated that data breaches could be costing the healthcare industry $6.2 billion over a two-year time span.[4] 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 that cyberattacks are the leading cause of data breaches in healthcare.

Ransomware is now more prevalent than ever. There have been more than 4,000 ransomware attacks daily since early 2016.[5] Just as with any other type of breach, both covered entities and business associates need to ensure HIPAA rules and regulations are followed to prevent, as well as recover from a ransomware attack and other cybersecurity-related concerns.

THE HIM PROFESSIONAL'S ROLE

HIM professionals are responsible for the overall confidentiality and integrity of health information and play an important role in controlling its availability, access, use, and disclosure. Strong collaborative relationships with senior leadership and all those within an organization are crucial to ensure compliance and to prevent impermissible access and/or disclosure of PHI.

HIM professionals must work with all stakeholders to ensure workforce members, and those working on behalf of the organization, as defined by HIPAA, are educated and trained. Adequate policies and procedures for the overall investigation and management of incidents/violations/breaches must also be developed and implemented.

Some states have unique statutes that may at times compete with federal rules, and sufficient knowledge in both state and federal rules pertaining to breaches is imperative. This toolkit does not address the differences between individual state and federal requirements. An organization should consult with its specific state statutes for further guidance.

Hacking and cybersecurity-related incidents are on the rise, causing an increase of PHI breaches. it is crucial that organizations have strong cybersecurity programs in place and HIM professionals, including but not limited to security officers, play a critical role in breach prevention.

DEFINING A BREACH: INCIDENT/VIOLATION/BREACH

The topic of breaches has pervaded the media. Breaches exist in all types and sizes and can occur in the smallest and largest of organizations. Due to the media focus on breaches, the terms *violation*, *incident,* and *breach* are used interchangeably; however, each has its own distinct meaning.

WHAT IS 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.

WHAT IS A VIOLATION?

A ***violation*** of the HIPAA Privacy or Security Rule occurs in instances where unsecured PHI was acquired, used, and/or disclosed in a manner not permitted by the rule. Under the Breach Notification rule, an entity is required to presume the violation to be a breach unless one of the three exceptions applies 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. Because these types of violations are presumed to be a breach, it is necessary for the organization to take appropriate steps to mitigate the issues and meet compliance with all breach notification and privacy rules or organizational policy requirements (where applicable).

WHAT IS A BREACH?

A ***breach*** is defined 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*" in 45 CFR 164.402. 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 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; and
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.[6]

The final rule identifies four factors that make up a breach risk assessment to include, at a minimum (See Section V for details and recommended practices for performing a breach risk assessment):

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

A covered entity's or business associate's analysis of the probability that PHI has been compromised following an impermissible use or disclosure must address each factor discussed above.

Criminal cyberattacks are a leading cause of data breaches in healthcare. It is important to note that HHS has published guidance on ransomware describing under what circumstances a ransomware attack could be considered a breach.[7] The guidance states that when electronic protected health information (ePHI) is encrypted as a result of a ransomware attack—in other words, the criminals encrypted the ePHI--a breach has occurred. The ePHI encrypted by the ransomware is acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA privacy rule. Unless the covered entity or business associate can demonstrate there is a "… low probability that the PHI has been compromised," based on the factors set forth in the breach notification rule, a breach of PHI is presumed to have occurred. The guidance goes on to describe that organization would then continue to follow breach management processes and rules in evaluating the probability that the PHI has been compromised.

RESPONSIBILITY AND ACCOUNTABILITY: COVERED ENTITIES/ BUSINESS ASSOCIATES

Once a breach has been discovered, the covered entity is ultimately responsible for ensuring that the breach notification process has been completed and that all affected individuals, the Secretary of HHS, and in certain circumstances, the media, have been notified in accordance with the requirements of the breach notification rule. Notification to the affected individuals must be provided without unreasonable delay and no later than 60 calendar days following discovery of a breach or when, by excercising reasonable diligence, the breach would have been known to the covered entity. BAs, upon discovery of a breach, must notify the covered entity without unreasonable delay. Additionally, subcontractors now have the responsibility to inform their contracted business associate of a breach, who in turn is responsible for notifying the covered entity.

Note: Organizations must take into consideration whether or not an agent relationship exists with the BA. An agent relationship will change the date of discovery. Refer to the Federal Common Law on agency and section 160.402 of the HITECH Final Rule for more information on the requirements of an agent.

Responsibilities of the Covered Entity

Once the breach is discovered, the covered entity must notify individuals of the breach without unreasonable delay and not later than 60 calendar days from the discovery of the breach, except in certain circumstances where law enforcement has requested a delay. In addition, if the covered entity discovers that a breach affects more than 500 residents of a state or jurisdiction, it must provide notice to prominent media outlets serving the state or jurisdiction. In addition to notifying affected individuals and the media (where appropriate), and the breach has affected more than 500 individuals, covered entities must notify the Secretary by visiting http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html) and completing an electronic breach form. If the breach affects fewer than 500 individuals, the covered entity may aggregate breaches and notify the Secretary annually, but no later than 60 days after the end of the calendar year in which the breaches occurred. Details of notification will be provided in Breach Section Notification of this toolkit.

Responsibilities of the Business Associate

1. The Breach Notification Rule (section 164.410) requires BAs to provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. The 60-day time period is the same length of time for both the CE and BA; therefore, it is recommended that the business associate agreement with the covered entity clearly define what constitutes timely notification of the business associate to the covered entity. This reporting period should be less than 60 days to allow the CE enough time to be compliant with their 60-day notification obligation. HHS, in its sample business associate agreement (see http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html), states that "the parties may wish to add additional specificity regarding breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS **Office for Civil Rights (OCR)**, and potentially the media, on behalf of the covered entity."

Business Associate Agreements

The ***business associate agreement (BAA)*** provides satisfactory assurances, in writing, of the BA's commitment to appropriately safeguard PHI that is created, received, maintained or transmitted on behalf of the covered entity. The contractual agreements established between the covered entities, business associates, and subcontractors are key to defining a breach response plan with the business associate and covered entity.

The BAA may also serve as a mechanism for ensuring that business associates and associated subcontractors are in compliance. CEs are encouraged to include verbiage in their agreements that describes how the BA may achieve compliance with HIPAA regulations and request documented evidence of internal/external audits, risk assessments, and mitigation efforts to monitor the business associate. For instance, a CE might add language that prohibits offshore work or international outsourcing to further ensure the BA is safeguarding PHI.

The following provisions for breach notification from the BA to the CE should include, at a minimum:

- Definition of a breach and when a breach is discovered
- Statement that the BA will report to the CE any use or disclosure of PHI, including breaches of unsecured PHI as required at 45 CFR 164.410, and any security incident of which it becomes aware. See HHS examples of contract provisions at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.
- Definition of when the BA should notify the covered entity upon discovery of a breach. For example, a CE may define the period of time not to exceed a certain amount of business days (i.e., five days, 10 days, etc.) It may be appropriate to consider requiring the BA to provide an initial verbal report within a reasonable time frame following the discovery with allowances of more time for the BA to follow up with a written, comprehensive report
- Definition of what should be reported to the CE. For example, the identification of each individual affected by the breach as well as any information required by the CE for its notification to affected individuals
- Statement describing the responsibility of the business associate/subcontractor to ensure compliance with HIPAA regulations by completing internal/external audits and risk assessments and regularly reporting results/mitigation efforts of such audits to the covered entity
- Description of how to ensure compliance by the business associate. Examples might include:
  - » Facilitating secure exchange beyond the **firewall** for safe transfer and exchange of electronic PHI which includes file transfer, data translation, and other types of interactions through defined technical safeguards
  - » Adhering to organization policies established by the CE that safely govern the flow of information between the CE and the BA, which include access and transmission controls

INVESTIGATION AND MITIGATION

DISCOVERY OF A POTENTIAL BREACH

Once a potential violation has been discovered, the entity must first substantiate that the incident was in fact a violation of the HIPAA Privacy Rule. Organizations make that determination by collecting the facts of the incident and analyzing the findings against the requirements of the rule. If the PHI was acquired, accessed, used, or disclosed in a manner not permitted by the rule, a violation is automatically presumed to be a breach unless it meets one of the three exceptions previously noted.

To ensure the organization is conducting investigations as required, it is important that the organization identify a process for reporting all potential violations. The reporting should include all privacy complaints from patients, families or others, impermissable access and/or disclosures of PHI to outside parties, incidents in which PHI was mailed, faxed, handed, etc., to the wrong recipient (even if this was purely an unintentional error), and inappropriate internal access or use of PHI (i.e., discovered via routine EHR access audit). Additionally, all security incidents including ePHI, especially those including suspected ransomware incidents, should be included in the reporting process. Each of these incidents is potentially a violation of the HIPAA Privacy Rule and therefore subject to a breach investigation.

LOGGING AND TRACKING INVESTIGATIONS

Once a potential breach is discovered and the investigation process begins, it is important that the covered entity or business associate log and track their cases under investigation. Logging investigations is simply the process of identifying cases the organization investigates. This can be as simple as a spreadsheet listing the cases as they are discovered, or more sophisticated software designed to facilitate the investigation process. Logging a case means opening up the documentation of each new case and beginning to capture the details. Each organization can decide how they would like to log and track breach investigations. There is no specific HIPAA requirement that defines this. This allows each organization to create a process that works best for their environment, structure, and workflow.

There are multiple reasons for logging and tracking investigations. Primarily, logging a case as soon as it is discovered will provide a method for monitoring timeliness of the investigation so that critical breach notification deadlines are not missed. This is especially important if the organization has investigations conducted by multiple individuals. Logging case details also provides the organization with valuable information that can assist with trending breach investigation activity. If the organization's logging captures and categorizes the right details such as types of violations, the information collected can be trended to help the organization identify problem areas useful for breach prevention efforts and HHS year-end reporting for breaches involving fewer than 500 individuals.

Although this process will not be the same at every organization, each organization should document their process for logging and tracking investigations in a policy and procedure. This will ensure there is no ambiguity on how, when, and by whom the process should be completed.

BREACH INVESTIGATION PROCESS

Internal Investigation Plan

The organization should develop an organization-wide general policy and plan for conducting investigations. The investigation policy will address specific steps that should be followed when conducting an internal investigation. Organizations should consider developing special investigation processes for potential breaches involving 500 or more individuals, as these breaches generally will have a greater impact on the organization. Some guidelines to consider for any type of breach, large or small, include:

- Establish a breach response team or designate individuals responsible for conducting breach investigations
- Investigate each incident swiftly and completely
- Develop corrective action steps including determining appropriate work force sanctions
- Conduct review to identify any potential problem processes
- Follow through with all required legal obligations

Breach Response Team

Composition of the breach response team will vary depending on the size of the organization and the type or size of the breach under investigation. For instance, breach investigations for incidents that impact a single or small number of individuals may be easily handled by a smaller team, while a large breach may be best managed with an extensive team of the organization's representatives. Small breaches might well be investigated by the privacy officer in collaboration with the operational leader responsible for the department involved in the breach, with the addition of a human resources representative if a breach involves a workforce member and warrants corrective action. For larger breaches, a cross-functional leadership team may be necessary to manage the breach investigation and related activities that are associated with a large breach. Potential representatives for a large breach response team may include:

- Privacy officer
- Chief compliance officer
- Security officer and appropriate IT representatives when applicable for ePHI breaches

- Operational leaders
- Risk management /legal /outside legal counsel
- Communications
- Cyber-insurance claims manager
- Human resources
- Loss prevention
- Health information management professionals
- Information governance leader

In general, some incidents may be straightforward and easily resolved. However, in the case of willful intent or complex cases involving large number of individuals including fraud and abuse violations, legal counsel involvement is advisable considering the subsequent risk and impact to the organization. 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. One of the most important steps in conducting internal investigations effectively is to identify a potential violation of the law. An organized series of steps that can be followed during an investigation will help provide consistency and objectivity, and avoid leaving out any key procedures. The administrative requirements of the 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. The following is an overview of a thorough investigation process:

- Collect and assemble all facts of the potential breach
- Describe and record specifically who, what, when, where, why and how the situation occurred
- Determine who is impacted (whether one or many individuals) and what PHI is potentially compromised
- Analyze and evaluate all the facts objectively to determine whether or not an impermissible access, use, or disclosure of PHI can be substantiated. Documentation must support the decision. For example, ransomware attacks must be carefully reviewed, including forensic analysis, to determine if a breach has occurred
- If a violation is substantiated, outline the remediation actions to be put in place, including mitigation, sanctions, education, and prevention
- Assess what notification processes must be made according to the breach notification rule
- Prepare reports, logs, and other required documentation and communications (internal and/or external)

Mitigation

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 covered entity 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. Timely mitigation may lessen the risk to the PHI, so be sure to take action quickly. Every mitigation process is likely to include an investigatory review of current privacy and security protocols involved in the incident. Mitigation steps may include:

- Review of security system and audit alerts to potential internal and external issues
- A forensics response process to preserve information needed during investigations
- Data recovery processes as well as technical solutions to respond swiftly in the case of information compromise

Mitigation means that the organization is taking steps to lessen the negative impact of the impermissible access, use, or disclosure with a goal to re-secure the PHI and obtain strong assurances that the information will not be further used or disclosed. Some mitigation considerations:

- For impermissible disclosures, mitigation should include attempts to recover or ensure the recipient has destroyed the PHI, and written confirmation of destruction
- Following any impermissible access, use, or disclosure obtain the recipient's assurances that the PHI will not be further used or disclosed. Obtaining written assurances, such as through a confidentiality agreement, strengthens the mitigation
- For incidents involving electronic PHI (ePHI), mitigation might include technical procedures such as remote wipe command capability for mobile devices

Where ransomware has accessed PHI, the organization may wish to consider the impact of the ransomware on the integrity of the PHI.[8] Frequently, ransomware, after encrypting data it was seeking, deletes the original data and leaves only the data in encrypted form. An organization may be able to show mitigation of the impact of a ransomware attack affecting the integrity of the PHI through the implementation of robust contingency plans including disaster recovery and data backup plans. Additionally, identifying whether the data has been exfiltrated (illegally copied) is another way to determine the extent to which the risk to PHI has been mitigated.

Risk Assessment of Breach

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:

- 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

In cases of ransomware, entities are encouraged to consider additional factors, as needed, to appropriately evaluate the risk that the PHI has been compromised. If, for example, there is a high risk of unavailability or degradation of integrity of the data, such factors may indicate compromise.[9]

Refer to section V for details and recommended practices on performing a breach risk assessment.

Education and Prevention

Before concluding an investigation, the organization should address education and prevention. Refresher training on policies and procedures relevant to the type of violation should be required for the individual(s) who caused the violation, keeping in mind that the entire department may need to be retrained. Additionally, leaders responsible for the area where the violation occurred should be required to review department processes to determine if any improvements should be implemented to prevent recurrence.

Investigation Considerations

As discussed earlier, the investigation process includes analyzing and evaluating all the facts objectively to determine whether impermissible access, use, or disclosure of PHI can be substantiated. There are many types of violations where it can be clearly established that a violation did or did not occur. For example, an audit trail will provide documentation of improper access to a record by an individual. Furthermore, an individual who was unauthorized to access such records may return documents containing PHI that were clearly disclosed to them in error. These breach determinations are straightforward and leave no doubt. However, sometimes there are situations where an individual makes a complaint where the allegations are only hearsay. In the case of hearsay, an individual might claim that an employee verbally disclosed PHI about them in public, but a subsequent investigation produces no facts to back up that claim. It is important that an investigation remain objective and factual without accepting statements from the individual that cannot be substantiated. Often these situations can only result in a determination that the violation is unsubstantiated and therefore no breach has occurred. This doesn't necessarily mean the same as conclusively determining that "no violation" has occurred, but it may be the only possible result. Consider careful documentation when investigating events that include:

- Describing how the potential breach was identified
- Reporting all investigation processes used
- Documenting a timeline of all individuals who were interviewed
- Reviewing all audit materials used during the investigation

Conducting a Breach Investigation Involving 500+ Individuals

Breaches that impact more than 500 individuals require protocols above and beyond regular breach investigations. Successfully managing a large breach requires an organizational incident response plan involving multi-department collaboration. Besides the usual breach investigation procedures required for any breach, a large breach often includes additional activities such as an internal and external communication plan or coordination with cyber-breach insurance, mail distribution, call center, and identity protection services. Some key tips for managing a large breach investigation:

- Identify a breach response team in advance to include the key individuals who will oversee and direct the investigation (see "Breach Response Team" section)
- Prepare a written incident response workflow depicting the high-level organization activities that may occur during a large breach investigation. A "swim lane" workflow diagram is an effective way to display the sequence of activities, responsibilities, and accountabilities
- Create detailed check lists to itemize the steps that must be executed for a compliant breach management and notification
- Set up service contracts/business associate agreements in advance with vendors whose services may be required as part of a large breach notification (i.e., call center, mail distribution vendor, identity protection services, outside legal counsel)
- Plan for daily breach response team calls to discuss the status of the investigation, identify action items, and plan next steps
- Set up a master calendar with deadlines for key activities that need to occur. A large breach has many activities occurring simultaneously and it is important to not lose sight of upcoming target dates

ORGANIZATION ENFORCEMENT

Addressing sanctions and holding employees accountable is an essential component of an investigation. For each incident that involves a substantiated violation, the organization should take steps to identify all members of the workforce that were involved, when possible, and then apply sanctions appropriate to the violation. Every covered entity or business associate must develop and document a sanction policy for the organization. The sanction policy will need to explain how appropriate sanctions will be applied against anyone in the organization's workforce who does not comply with HIPAA rules and/or the organization's privacy and security policies.

Organizations should classify different sanctions depending on the nature of the privacy or security occurrence. Employee motivation or intent may also be factors used to classify sanctions. Classification will help the organization create a standard for determining corrective action. Sanctions or other organizational policies should also address nonretaliation actions against workforce members who self-report their own infractions. This is not only required by HIPAA, but also necessary to support and encourage voluntary self-disclosure.

CATEGORIES OF OFFENSES

Minor Offense—Education and/or Coaching; Progressive Discipline	
Definition	Examples
Generally a minor offense will be one where the breach was not intentional.	Accidentally e-mailing unsecured PHI Discussing patient information in a public setting Placing confidential trash in a regular trash bin
Serious Offense—Written Warning Up to and Including Discharge	
Definition	Examples
Generally a serious offense can be one where the breach was not intentional, or it was intentional with no malice or personal gain.	Unlawful or unauthorized access, use, disclosure, viewing, and handling of confidential information but without the intent to cause harm Repeatedly being careless with PHI Frequently leaving a workstation unattended while it is logged on to confidential information Sharing passwords
Major Offense—Immediate Discharge Due to Severity of Offense	
Definition	Examples
Generally a major offense is one where the individual is at risk for legal action, and is carried out in a dishonest manner without regard for the organization or the patient, and involves malice or financial or personal gain.	Unlawful or unauthorized access, use, disclosure, viewing, and handling of confidential information with willful intent or to intentionally cause harm to a patient, the organization/covered entity, or to another individual Using confidential information for identity theft or to commit fraud, or for personal gain Intentional alteration or destruction of confidential information Gross violation of HIPAA or any other federal or state law protecting the confidentiality of information

Courtesy Tom Walsh Consulting, LLC

By following these principles, organizations can position themselves for consistent unbiased outcomes. The policies should:

1. Be created and approved in the same process that all other [sanction] policies and procedures are created and approved within the organization
2. Be designed to accommodate future regulations and standards
3. Be consistent with other policies and procedures that are already in place in the organization, as well as, BAAs, contracts, and bylaws
4. Be available for the entire workforce to review
5. Speak to the breach notification sanctions process if an unauthorized access, use, disclosure, or destruction is discovered

6. Explain investigations made by whistleblowers or crime victims as possible nonviolations
7. Discuss that organizations are prohibited from intimidating, threatening, or retaliatory acts against anyone in the workforce who files a complaint either with the organization or with the Secretary of HHS
8. Involve human resources to ensure policies and sanctions are consistent with the organization's corrective action policies
9. Speak to state and federal regulations regarding retention of significant sanctioning documentation
10. Consider the scope and size of the breach in combination with the intent of the violation.

BURDEN OF PROOF/DOCUMENTATION

Documentation is a requirement of breach investigations. The HIPAA Privacy Rule §164.530 Administrative Requirements specify that covered entities are required to document all complaints received and their disposition, as well as any sanctions that are applied. The HIPAA breach notification rule §164.414 ***burden of proof*** standard additionally provides that covered entities have the burden of proof to demonstrate that all notifications were made or that an impermissible use or disclosure did not constitute a breach (such as by demonstrating through a risk assessment that there was a low probability that the PHI had been compromised).

To meet the burden of proof and ensure compliance with the rule, it is important to document and retain as required by HIPAA (dependent upon the nature of the violation and investigation) the following:

- All findings and information pertinent to the investigation
- The risk assessment and all associated documents demonstrating that all factors were evaluated and how the potential breach was determined to be a "low probability" that PHI has been compromised
  - » Assurance of destruction by the unauthorized recipient
  - » Assurance that the PHI will not be further used or disclosed by the unauthorized recipient

Unless the risk assessment demonstrates low probability of a breach, then documentation of all notifications made must also be maintained to ensure compliance with this requirement, which includes retaining a copy of the notification to HHS. Documentation provides the safeguard for the CE or BA in the event the determination is called into question.

The organization's choice of forms or templates used to document investigations should aid in ensuring a compliant and complete investigation. Design forms and templates so that the components of a thorough investigation (mitigation, sanctions, education, prevention) must be documented. If forms only contain open-ended narratives, the person documenting the investigation may not remember to address those sections specifically. Forms that include specific sections for documenting mitigation, sanctions, education, and prevention will facilitate compliant investigations and consistent documentation. When designing investigation forms, also consider including sections to collect data that will be needed for notification and reporting (refer to appendix B for a sample checklist).

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 (as defined by HIPAA). It is critical that the determination is timely and accurately so the appropriate actions can be taken. 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, 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 (both the person who inappropriately accessed as well as the individual whose PHI was inappropriately accessed or disclosed, to name a few).

For guidance and recommended practices on performing a breach risk assessment, refer to the practice brief excerpt below.

AHIMA PRACTICE BRIEF (EXCERPT): PERFORMING A BREACH RISK ASSESSMENT

Evaluating for Low Probability of Compromise

After a breach has occurred, the performance of a documented risk assessment provides a consistent method for determining whether the PHI has been compromised.

This risk assessment must consider at least the following four factors:

1. Nature and Extent

The first factor to consider is the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

The probability of compromise increases when the information is of a sensitive nature or the type of identifiers exposed increase the risk of identity theft, financial fraud, or improper use of the information. If the amount and type of PHI used or disclosed is minimal then the probability may decrease.

The following list of questions assist in evaluating the "nature and extent" of the PHI involved:

- Which patient identifiers were used or disclosed? Does the combination of identifiers used or disclosed increase risk? Are there particular identifiers such as a Social Security Number (SSN) that raise concerns?
- Does the PHI used or disclosed contain a sensitive diagnosis? (i.e., substance abuse, mental health, sexually transmitted disease, HIV, cancer)
- Does the amount of PHI used or disclosed increase the risk?
- Does the use or disclosure reveal the PHI of a well-known individual?
- Does the PHI used or disclosed include sufficient indirect patient identifiers that could make re-identification of the individuals possible?

The goal of evaluating this factor is to determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipients' own interests.

2. Unauthorized Person

The unauthorized person who impermissibly used or to whom the PHI was disclosed is relevant to the risk assessment to assist in determining the probability for compromise. For example, if the recipient is another entity regulated by the HIPAA Privacy and Security Rules or other privacy laws, there may be a lower probability that the PHI has been compromised since the recipient is obligated to protect the information. On the other hand, if the unauthorized person is not a covered entity, the probability for compromise may be increased, especially if the recipient's actions are untrustworthy or unpredictable.

Questions to consider in this portion of the risk assessment include:

- Does the unauthorized recipient have obligations to protect the privacy and security of the disclosed information such as a business associate or another covered entity?
- Is the recipient a member of the organization's internal workforce or a business associate to ensure that the PHI will not be further used or disclosed?
- Does the recipient have a relationship with the individual where they are likely to act in the individual's best interest?
- Is there additional risk if the recipient likely knows the subject of the PHI?
- If the recipient impermissibly used the PHI, what was their purpose or motive for doing so? (i.e., unintentional or inadvertent error, intentional self-serving, malicious, or harmful intent)
- What was the attitude and demeanor of the unauthorized recipient? Were they cooperative and willing to help secure the PHI? Were they also concerned about protecting the PHI? Was contact initiated immediately or did it appear there was reluctance for cooperation as leverage for something else [for own best interests]?
- Was the recipient an unintended recipient or did the recipient seek out the information?
- If only indirect identifiers were disclosed, does the recipient have the ability to re-identify the PHI?
- Is it believed that the PHI was taken with intent to use or sell?

The goal of evaluating this factor is to determine the probability as to whether the recipient might further use or disclose the PHI in a manner adverse to the individual or for the recipient's own interests.

A recipient who did not seek out the access, who is cooperative and willing to quickly return information, who did not have any adversarial relationship to the individual or likelihood of personally knowing the individual, could be considered a low-risk recipient.

3. Acquisition/Viewing of PHI

Covered entities must determine whether or not the PHI was actually acquired or viewed or whether there was an opportunity for the PHI to be acquired or viewed. The probability of compromise is lowered only if the opportunity existed for the PHI to be acquired or viewed but the PHI was not actually acquired or viewed. For example, a billing statement sent to the wrong address that is returned unopened would be considered PHI that was not actually viewed. In contrast, if the billing statement was opened and the recipient called to notify the covered entity, it would be considered acquired and viewed.

Questions to consider in this portion of the risk assessment include:

- Was the PHI actually acquired or viewed by an unauthorized person?
- Is it possible to demonstrate that the disclosed PHI was never accessed, viewed, or acquired?
- If an electronic device was involved, does forensic analysis show that the PHI was accessed, acquired, viewed, transferred, or compromised?
- If ePHI is involved, what does the audit trail indicate? What actions (i.e., print, view) were taken? What parts of the record were accessed?

4. Extent Risk Has Been Mitigated

Quickly mitigating any risk to PHI that was impermissibly used or disclosed, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed or will be destroyed, may lower the probability that the PHI has been compromised. Questions to consider in making this determination include:

- If the recipient was a CE or other reliable business bound by privacy obligations (i.e., BAs, banks, or attorneys), was verbal confirmation given and documented that PHI was destroyed?
- If the recipient was not a CE or other reliable business otherwise bound by privacy obligations, was written confirmation of destruction obtained?
- If the recipient was an employee who impermissibly used PHI, was a statement of assurance obtained attesting that PHI will not be further used or disclosed?
- Has satisfactory assurance been obtained from the unauthorized recipient that the disclosed PHI will not be further used or disclosed or will be destroyed? Has an effective mitigation strategy been implemented such that further unauthorized disclosures are extremely unlikely?
- Was the PHI returned in a timely fashion and intact?

The goal in evaluating this factor is to determine how thoroughly and quickly the PHI involved has been secured following the impermissible use or disclosure. Once all factors have been reviewed, the CE must then evaluate the overall probability that the PHI has been compromised by considering all the factors in combination. Other factors may also be considered where necessary.

SCORING MATRIX FOR DETERMINING PROBABILITY OF COMPROMISE

The probability that a breach of PHI with associated risk has occurred can be scored by evaluating the likelihood and potential impact that the information has been compromised.

Likelihood*	Impact**		
	Minimal 10	**Moderate 10**	**Severe 100**
High 1.0	Minimal 10	Medium 50	High 100
Medium 0.5	Minimal 5	Medium 25	Medium 50
Low 0.1	Minimal 1	Low 5	Low 10

*Likelihood

- **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

**Impact

- **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[10]

DETERMINING LOW PROBABILITY OF COMPROMISE

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation. A completed risk assessment is a tool that can assist in determining the extent of the potential threat and the risk associated with it. In an effort to determine if there is a "low probability" that PHI has been compromised, an objective scoring tool may be used. Taking the four factors described into consideration, the probability can be scored by evaluating the likelihood and potential impact that the information has been compromised.

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

Breach Risk Assessment Tools:

See Appendix C for a sample tool that may be utilized to assist in scoring each factor and documenting the risk assessment.

See Appendix D for a sample case using Appendix A and the scoring table above to help demonstrate low probability of compromise.

See Appendix E for a decision tree diagram that follows the workflow from the point an incident is reported through the actions necessary for compliance.

The full practice brief can be found in the AHIMA Body of Knowledge at: library.ahima.org/doc?oid=107071.

BREACH NOTIFICATION

A successful breach notification process ensures the prompt notification to the individuals whose PHI has been breached. Once a determination that breach notification is required, §164.404 of the rule requires an organization to notify each individual whose unsecured PHI has been or is reasonably believed by the organization to have been accessed, acquired, used, or disclosed as a result of a breach.

While a breach notification may be provided by various methods, the rule does not indicate how long a breach notification letter should be; however, it must include the following elements at a minimum, and it should not include extraneous information that would detract from the message.

Example: The rule clarified that some breaches involving more than 500 individuals who are residents in multiple states may not require notice to the media. For example, if a covered entity discovers a breach of 600 individuals, 200 of whom reside in Virginia, 200 of whom reside in Maryland, and 200 of whom reside in the District of Columbia, the breach did not affect more than 500 residents of any one state or jurisdiction, and as such, notification is not required to be provided to the media pursuant to §164.406. However, individual notification under §164.404 would be required, as would notification to the Secretary under §164.408 because the breach involved 500 or more individuals.[11]

In the event a breach impacts individuals across multiple states, notification should be provided according to the number of individuals impacted by state.

REQUIRED AND CUSTOMIZABLE ELEMENTS IN A BREACH NOTIFICATION LETTER

The breach notification letter (see Appendix F for sample letter) must contain five required elements addressed in a customized manner according to the situational circumstances and consisting of:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known
2. A description of the types of unsecured PHI that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, diagnosis, or disability code)
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach
4. A brief description of what the organization is doing to investigate the breach, to mitigate harm to the individuals, and to protect against any further breaches
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address[12]

If appropriate, the organization may include other customized information, including:

- Information about steps the organization is taking to prevent future similar breaches
- Information about sanctions the organization imposed on workforce members involved in the breach. Identity of workforce members should be on a need-to-know basis according to organizational policy
- Consumer advice directing the individual to review account statements and monitor credit reports
- Recommendations that the individual place a ***fraud alert*** on their credit card accounts, or contact a credit bureau to obtain credit monitoring services, if appropriate
- Contact information for credit reporting agencies, including the information needed for reports for ***criminal investigation*** and law enforcement
- Contact information for national consumer reporting agencies
- Information about steps the organization is taking to retrieve the breached information, such as filing a police report (if a suspected theft of unsecured PHI occurred)
- Whether or not criminal complaints have been filed
- Whether or not there was a delay in notification because of forensic investigations
- Information regarding law enforcement contacts
- Consumer advice on how to report suspected identity theft to law enforcement and the Federal Trade Commission
- The toll-free telephone numbers, addresses, and website addresses for the Federal Trade Commission, the office of the attorney general, and the state police or consumer protection agency
- Information about steps the organization is taking to improve security to prevent future similar breaches
- Other discretionary data[13]

It should be noted that organizations may need to comply with various notification requirements with other federal laws including Title VI of the Civil Rights Act of 1964, the Rehabilitation Act of 1973, Section 504, and the Americans with Disabilities Act of 1990. The urgency of circumstances may require a notification letter be sent before the investigation is complete. An organization may determine whether or not there is a need to send a follow-up letter when more information is known. HHS emphasizes that the exact or sensitive information breached should not be listed in the notification letter. The final rule does not direct the provider to release the names of the individuals responsible for the breach. A decision must be made whether to list both the covered entity and business associate in the information provided in the letter when a business associate is involved.[14]

Lastly, the organization may be required to include other elements in the letter in accordance with specific state laws, other applicable federal guidelines, and its own organizational policy.

PLAIN LANGUAGE REQUIREMENT

The rule states that the individual notification letter should be presented at an appropriate reading level, written in plain language and able to be easily read by the individual, their personal representative, or another individual making healthcare decisions on behalf of the individual.

METHOD OF DELIVERY

The rule requires that the written notification be made by first-class mail to the individual. If the organization is aware that the individual is deceased and knows the address of the next of kin or personal representative of the individual, written notification shall be made by first-class mail to either the next of kin or personal representative of the individual at their last known address.[15] If specified as the preferred method, the notice may be sent electronically as long as the individual has not withdrawn their agreement. In cases that are deemed urgent and require immediate notice, because of the possibility of imminent misuse of unsecure PHI, the notice may be provided to the individual by telephone or any other alternative means in addition to the direct written notice. Face-to-face notification may be required, particularly when the individual has received highly confidential services such as substance abuse or mental health services.

SUBSTITUTE NOTICE

If there is insufficient or out-of-date contact information that precludes written notification to the individual, next of kin or personal representative, a substitute form of notice (see Appendix G for sample notices and statements) reasonably calculated to reach the individual, next of kin or personal representative, must be provided. However, the substitute notice does not need to be provided if there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of a deceased patient. In those cases, the following guidelines apply:

A. Fewer than 10 individuals

1. If there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, by telephone, or by other means.
2. Posting a notice on the organization's website or at another location may be appropriate if there is no current contact information, so long as the posting is done in a manner that is reasonably calculated to reach the affected individuals.

B. Ten or more individuals

1. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice must:
    a. Be in the form of either a conspicuous posting for 90 days on the home page of the organization's website or a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.
    b. Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether his or her unsecured PHI was included in the breach.

C. Web posting

1. If the organization uses a hyperlink on the home page to convey the substitute notice, the hyperlink should be prominent so that it is noticeable given its size, color, and graphic treatment in relation to other parts of the page and should be worded to convey the nature and importance of the information to which it leads.

D. Media

1. A substitute notice in major print or broadcast media must be used in geographic areas where the individuals affected by the breach likely reside. In a rural area, the local newspaper may suffice. In a metropolitan area, a newspaper serving the entire area or the entire state may suffice.

E. Additional notice in urgent situations

1. If the organization believes it is urgent to notify the individuals of the breach because of possible imminent misuse of unsecured PHI, the organization may notify individuals by phone or other means as appropriate. However, a written notice or substitute notice, as described above, must also be made.
2. If the patient is deceased and the next of kin or personal representative cannot be reached, then no further action is needed.

Note: Substitute notice does not apply to situations where the identity of the individuals whose PHI has been compromised is unknown, such as situations where a theft of PHI has occurred, and it is unknown specifically whose PHI was taken. These situations do not qualify as "insufficient contact information," triggering substitute notice. In these cases, the organization will need to determine the individuals whose PHI may have been compromised and provide individual breach notifications accordingly.

MEDIA NOTIFICATION FOR BREACHES INVOLVING MORE THAN 500 RESIDENTS

If there is a breach of unsecured PHI involving more than 500 residents of a state or jurisdiction the organization must notify prominent media outlets serving that state or jurisdiction. This required media notice is intended to supplement the direct written or substitute notice and may not be used as the sole method of notifying the individual of a breach.

The required notice to the media must include the same information required in the notice to the individual and must be given within the same timeframe. HHS states that it expects that most organizations will provide notification to the media in the form of a press release.

TIMELINESS OF NOTIFICATION

An organization must notify the individual without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach. However, organizations might consider setting their own deadline (i.e., 30 days) to ensure ample time for meeting compliance and potentially lessen any penalties by HHS. The rule states that a breach is treated as discovered by an organization, as of the first day on which the breach is known to the organization, or by exercising reasonable diligence, would have been known to the organization. The rule further states that an organization "shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is a workforce member or agent "of the organization.[16] Organizations should conduct a review of state breach notification laws/regulations to determine whether the timeliness of notification varies from the federal rule.

Note: Organizations must take into consideration whether or not an agent relationship exists with the BA. An agent relationship will change the date of discovery. Refer to the Federal Common Law on agency and section 160.402 of the HITECH Final Rule for more information on the requirements of an agent.

DELAY DUE TO LAW ENFORCEMENT

Notification may be delayed due to law enforcement determination (section 164.412) that a criminal investigation would be impeded or that notification may cause damage to national security. If law enforcement provides a request in writing to delay notification, the organization must comply with the request for the time period specified. If provided orally, the request is valid for 30 days from the date of the oral request and may only be delayed further upon receipt of written request.

BREACH REPORTING

Covered entities and business associates are required to notify the 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 a breach impacts more than 500 individuals across multiple states, while there may be multiple media notifications, only one HHS report should be submitted.

For any breach affecting fewer than 500 individuals, covered entities and business associates are required to notify HHS annually. In most situations, the covered entity will complete the HHS notification process. However, a business associate may accept the reporting responsibility as outlined in a business associate agreement, for example. 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.

Note: Subsequent breach reports (regardless of size) may be submitted should more information become available to supplement the initial report.

The instructions for submitting a notice of a breach to the Secretary of HHS of unsecured protected health information and links to appropriate reporting web portals is located at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.

The OCR has established notification requirements for covered entities and business associates. Breach notification rule requirements can be located at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

It is important to note that many state regulations require more strict breach reporting requirements, so it is imperative to review regulations for the state within which the CE resides and regulations for the state in which the individual(s) resides.

OCR ONLINE BREACH REPORT ELEMENTS

Following a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred. The elements to capture in anticipation of reporting a breach to the Secretary of HHS are provided below. Refer to Appendix H for a sample worksheet on completing this report.

- Number of individuals affected by the breach
- Is this the initial report or an addendum to a previous report?
- Name of the CE, type of CE, address, name of contact person for the CE, contact phone number and e-mail for the contact person
- Name of the BA, address, name of contact person for the BA, contact phone number and e-mail for the contact person (if BA related)
- Date range for the breach
- Date range of breach discovery
- Approximate number of individuals affected by the breach
- Type of breach
- Location of breached information
- Type of PHI involved in the breach
- Brief description of the breach
- Safeguards in place prior to the breach
- Date(s) individual notice of the breach was provided
- Was a substitute notice required?
- Was it necessary to provide a media notice?
- Actions taken in response to the breach
- Attestation at time of electronic submission to the Secretary of HHS

ENFORCEMENT AND PENALTIES

The HIPAA rules address enforcement in detail. The Office for Civil Rights (OCR) is part of the HHS and is responsible for enforcing the HIPAA Privacy and Security Rules (45 CFR Parts 160 and 164, Subparts A, C, D, and E).

Breach notification may lead to various enforcement actions. Since the passage of HITECH and subsequent implementation of the HIPAA breach notification rule, OCR prioritized the investigations of reported PHI breaches affecting more than 500 individuals and imposed fines, penalties, and with increasing frequency, corrective action plans on the responsible organizations. Despite statutory authority to investigate all PHI breaches, OCR had primarily focused on large-scale breaches. However, in 2016 OCR announced an initiative to more broadly investigate smaller breaches with a plan to increase efforts to identify and obtain corrective action to address entity and systemic noncompliance related to small breaches.[17] Several enforcement actions triggered by smaller breaches have already been announced. Organizations should take note of this announcement and refocus their breach prevention efforts.

STATE ATTORNEYS GENERAL

State attorneys general were granted additional enforcement authority for protecting patient privacy rights under the February 2009 HITECH Act (part of the **American Recovery and Reinvestment Act or ARRA**). The attorneys general are impacted in several different ways. In addition to expanded enforcement authority in protecting patient privacy under HIPAA, the regulations also encourage increased use of electronic storage with the transfer of PHI. With the increased use of e-storage and transferring PHI electronically, there are increased opportunities for breaches of PHI, giving rise to instances in which state and federal privacy regulations and/or laws have been violated.

While HIPAA regulations can be complex, the HITECH Act strengthened and extended disclosure requirements and introduced the breach notification requirements. Attorneys general have the legal authority to bring civil suits in federal district courts on behalf of residents of their state; they've also been empowered to sue for injunctive relief and/or for damages.

NOTE: Any CE/BA who is under investigation by the OCR should consult with legal counsel to make certain all rights under HIPAA are preserved.

BREACH PREVENTION

As of October 2017, OCR had settled or imposed civil monetary penalties in 52 cases resulting in a total dollar amount of $72,929,182.[18] In 2017 alone, OCR either settled or imposed a civil money penalty on 10 organizations, for a total of $19,393,000, in cases ranging from $31,000 to $5,500,000. In fact, the first settlement of the year in the amount of $475,000 was specifically for failure to notify of a breach in a timely fashion.[19]

Considering the potential losses, healthcare organizations are discovering that breaches have severe and far-reaching consequences. The cost of these breaches can be staggering. Subsequently, this knowledge is driving organizations to invest resources in strong breach prevention efforts. Investing in the prevention of breaches may have a significant return on investment.

SECURITY IS KEY

Without a doubt, a strong security program is key to breach prevention. Prior best practices for a security program held that as long as ePHI is securely maintained or transmitted in accordance with OCR guidance, breaches could be prevented and mitigated. Incidents might still occur, but they would not rise to the level of a breach if the ePHI was rendered secure. However, the current rise in new types of malicious attacks, such as ransomware, has caused OCR to issue new guidance that requires careful consideration of additional factors in determining if the ePHI was exfiltrated, which would mean, even if encrypted, a breach may have occurred.[20]

Security alone will not prevent breaches, and human error is the most common factor in many breaches. Opening links in unsolicited emails often leads to a ransomware attack that breaches an organization's network and electronic systems. Failure to follow procedures, carelessness, or inadvertent mistakes can cause breaches involving other forms of PHI (i.e., document hand-off, misdirected faxes, failure to use a cover sheet).

There are certain steps an organization can take to foster an environment where strong breach prevention and recommended practices that reduce and mitigate violations are developed. Effective breach prevention relies on a comprehensive approach by employing several continuous practices in unison. Breach prevention is not just a back-end approach of educating one person after a violation. Breach prevention is a layered approach that needs to instill a culture within the organization. It involves leadership support and accountability, trending violations and breaches, communication, focused education, and monitoring.

With ransomware attacks on the rise, properly following all HIPAA security measures can help prevent ransomware attacks. HIPAA outlines the following security measures to reduce the risk to 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; and
- Implementing access controls to limit access to ePHI to only those persons or software programs requiring access.[21]

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 and thereby strengthen the program.[22]

LAYING THE GROUNDWORK WITH LEADERSHIP

Before breach prevention can be planned or initiated, an organization must first find ways to ensure it is receptive and ready to do its part. Lay the groundwork so there is a clear understanding that compliance is everyone's responsibility and there are consequences for noncompliance. By following these steps an organization can build a culture ready for breach prevention efforts.

To ensure sucess, start with gaining the support and buy-in needed from senior leadership to help ensure success. Senior leadership attention can quickly be attained by describing the enforcement climate under HITECH. An effective way to do this is by recounting some of the real-life stories of settlements, resolution agreements, OCR audits, breach notification, and other potential enforcement actions that are a real possibility for the organization. Besides the threat of strict enforcement, describe the impact of a privacy violation from the viewpoint of a patient whose PHI was compromised. Communicate the worry, concern, and life-changing impact a patient may experience. Help leaders understand the costs to the organization both financially and indirectly by the loss of reputation or patient trust. Once they understand the consequences of noncompliance, ask organization leadership for their support to ensure there are opportunities to regularly provide privacy and security education and updates and to hold departments accountable for cooperation with compliance efforts.

Once senior leadership is on board, take a similar message to department leaders across the organization. Identify the expectations of the leader and enlist their support to hold employees accountable when violations occur and to assist with education and monitoring efforts.

Continue the message to the front-line employees so they realize that as they handle PHI while performing their jobs, they will be held accountable for following the rules and are entrusted to safeguard the information.

The overall goal in laying the groundwork from the top down is to foster an environment where the importance of protecting the privacy and security of patient health information is strictly enforced. This is not just to mitigate financial consequences, but to maintain patients' trust and loyalty. The goal is to build a culture where every employee has a heightened awareness that PHI needs to be protected for the sake of the patient's privacy and for the protection and reputation of the organization. Each person needs to understand that when they access, use, or disclose anything involving PHI that they are handling something very valuable to the patient. It is an employee's ethical and moral responsibility to secure and protect PHI properly.

TRENDING VIOLATIONS AND BREACHES

Before breach prevention efforts can be fully implemented, a solid understanding of the violations and breaches that occur within the organization must exist. By trending investigation activity, the types of behaviors that cause violations can be identified and therefore help focus the right education more effectively.

To ensure comprehensive violation trending, the organization must make sure all potential HIPAA privacy and security concerns are reported. It is important to know what is happening in the organization not only to appropriately mitigate and follow the HIPAA breach notification rules, but also because an organization cannot prevent what it does not know is happening. Enlist the support of the department leadership to spread the message that reporting potential HIPAA issues is everyone's responsibility and that reporting is necessary for the organization's compliance. Provide the workforce with easy methods to report and identify the types of issues that should be reported. Stress to the workforce that all potential violations should be reported, even those not yet substantiated.

Data collection during the investigation process is key to trending activity. Information to trend and collect might include number of violations, number of reportable breaches, organization or department involved, type of violation such as disclosure or access, and behavior that caused the violation such as document handoff or misdirected fax. Consider formatting the investigation logging and tracking method or documentation forms to facilitate consistent data collection. The goal is to have enough detailed information to allow for proper analysis of what is happening in the organization. What types of violations are occurring, what specific behaviors are causing the violations, which violations are most likely reportable breaches, where are they occurring, which types of employee positions typically cause certain types of violations? Armed with that information, an organization can focus education more effectively to target problem areas.

COMMUNICATION

Once data is collected, it is important that the trends and statistics are communicated in ways that will create awareness and help further overall breach prevention efforts. Consider creating ***dashboards*** that display the data in meaningful ways that are easy to understand. For instance, a dashboard that displays a pie chart with the top five behaviors that cause violations can easily be used to communicate the organization's problem areas. A dashboard might also include a de-identified description of the reportable breaches or numbers of violations compared across quarters.

Communication is a key step toward breach prevention as it keeps awareness high and continually reminds leaders to examine what is happening in the departments for which they are responsible. Communication keeps HIPAA privacy and security in the forefront of leaders' minds so that they can see their departments from the viewpoint of privacy and security. A privacy or security officer cannot be monitoring operations everywhere; an organization needs well-informed leaders who must be the eyes and ears for privacy and security compliance within the settings they oversee. Use dashboards to create discussion within the organization at management meetings, compliance or other committee meetings, or in whatever forum where the audience might have a role in ensuring compliance. In addition to sharing the dashboard, highlight the behaviors that are causing the violations and reportable breaches and create a dialogue on how to further communicate the issues.

The overall goal of communication is to continuously bring privacy and security compliance back to the forefront of leaders' minds and of the organization. Unless it is the privacy or security officer, generally leaders in the organization don't see the workplace with "HIPAA eyes." Regular communication will help keep awareness high so that leaders can more easily spot behaviors or processes that might lead to violations, stop them before they occur, and promote early reporting of potential HIPAA incidents and violations.

POLICIES AND PROCEDURES

Policies and procedures are an important necessity to meet compliance with organizational process as well as federal and state laws and regulations. Policies and procedures set the tone and expectation of the organization on its workforce and others outside the work force (i.e., business associates and their subcontractors).

Every policy and procedure must follow a continuous life cycle of creation, approval (including senior leadership support), education and training, implementation, and review/update. Standard practice is usually advised for review and update (if needed) of policies at least once a year. However, updates should occur every time there is a change in organizational expectations, change in laws/requirements, or change in a system or process.

Finally, policies and procedures are only as strong as the education and training provided to the workforce to implement them. Education and training must be provided at all levels to instill a strong culture of compliance.

At a minimum, the following breach policies and procedures should be in place:

- Incident reporting
- Incident investigation
- Breach reporting
- Breach notification
- Sanctions
- PHI access, use, and disclosure
- Auditing and monitoring
- Information security
- Workforce training
- Minimum necessary

EDUCATION AND TRAINING

Education and training is a critical step for successful breach prevention. Education should be provided regularly and use different approaches.

- Training: At a minimum, annual training for all employees will provide employees with the basics and may serve as a refresher at that point in time, but it likely won't be enough to keep awareness high throughout the year. When providing annual training, create content that does not just rehash the HIPAA rules. Focusing annual training on the behaviors or scenarios that typically cause violations may be more effective in preventing breaches. Training should be provided as the need is identified and as changes are implemented.
- Focused education: Education that targets the behaviors that cause violations and breaches will be most effective in preventing breaches. When creating this education, the trending of violation information will be helpful in identifying what topics to address. Focused education content should be very brief and to the point. It should describe the type of violation, the behavior that causes it, the consequences of the violation, and a few short points as to what the employee can do to prevent the violation. Adding real-life stories or attention-getting introductions will increase interest. If focused education can be provided to a specific department in person, this presents an opportunity to engage the department in a discussion as to how protecting PHI and the training specifically relate to the work they perform. If it is not possible to provide the training in person to employees at the front line, deliver the education at the leadership level and distribute a handout to the leaders with an expectation that they share the information within their departments. Additionally, leaders can generate a discussion as to how their department could improve and prevent the breach. Focused education can also be posted as a monthly "focus on compliance" article on the organization's intranet. Ideas for focused training topics include, but are not limited to:
  - » Document hand-offs
  - » Speaking with family and friends
  - » Social media
  - » Verification of fax numbers
  - » Password management
  - » Use of encryption
  - » Safeguarding PHI
  - » Proper verification when speaking on the phone
- Education when a violation occurs: As part of conducting a thorough investigation, whenever a privacy investigation substantiates a violation or breach, education should be considered as part of the mitigation process. A good organizational policy is to require the employee who caused the violation, if known, to complete some privacy refresher training. Refresher courses and training should be focused specifically on the rule that was violated and any corrections that they need to make to prevent further violations. When providing refresher training following a violation, consider "the ripple effect." Just as a stone thrown into a pond causes a ripple to expand across the water, when educating one employee who caused a violation, take that opportunity to provide education to others who might potentially make the same mistake. For example, if an employee caused a breach by not following a specific rule, provide education to others in the department to ensure everyone is fully aware of the correct procedure. Depending on the type of violation, it is possible that same mistake could repeat itself on a widespread basis, and it is important to broaden the education across the organization.

PROCESS IMPROVEMENT

When trending violations, patterns may develop suggesting that a particular process or lack of process contributes to certain violations. Engage the organization's process improvement teams to help identify problem areas and develop process changes to aid in overall breach prevention. Even if an issue is not widespread enough to warrant a project team, require department managers to review all processes involved each time a violation occurs within their department. This can help to determine if process improvement could prevent future occurrences.

AUDITING AND MONITORING

Breach prevention is a continuous process. As staff and processes change, the potential exists for violations to occur and the organization must regularly monitor for problem areas that might lead to violations. A breach can be prevented whenever it can be caught as a problem waiting to happen. Here are a number of ways to accomplish that:

- Safeguard walkthrough: At various unannounced intervals, have leaders or privacy officers walk through the building and departments like a visitor. What PHI might they see or hear that they shouldn't? Corrective action should be performed on the spot to correct the potential issue.
- Identify staff who regularly walk through a building, such as security personnel, and train them to observe for lack of safeguards that might cause a breach, such as PHI left viewable on a screen, doors propped open that should be secured, or conversations that can be overheard. For example, some organizations use "Be HIPAA Aware" cards that the staff might leave in the department describing the issue they observed. "Be HIPAA Aware" cards (or cards such as these) are friendly reminders that a compliance issue was discovered and are meant to raise awareness to small safeguard issues that have been overlooked.
- Proactive electronic health record (EHR) auditing can be a good breach deterrent. Regularly audit for potential access violations and let it be known to employees that their access is monitored. If they know access is audited and reviewed, they might be less likely to access inappropriately.
- ***VIP Record*** Lockdown: Use system ***"break the glass"*** tools to lockdown records that might be accessed by the curious. The extra security may prevent inappropriate access.
- Compliance ***scorecards:*** A compliance scorecard is a tool organizations might use to measure various compliance activities. Just as organizations measure quality or patient satisfaction, they should consider measuring compliance activities and outcomes. A scorecard can be used to hold leaders accountable for participating in compliance activities and improving their outcomes. The scorecard would list the activities that are expected to be completed on a monthly or quarterly basis. The organization is then measured on whether it performed those activities or not and given either a pass or fail score. The leaders of the organization are then held accountable to ensure the site receives an overall "pass." The leaders in turn hold others who might be specifically responsible for tasks on the scorecard accountable. A scorecard is a very tangible reminder and incentive for monitoring compliance and ensures the sites are examining their own compliance. Scorecard measures that assist breach prevention efforts would include measuring reportable breaches, measuring the percentage of employees who completed annual training, or measuring education provided.

NOTES

1. 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.
2. Ziskovsky, Tracy. "2017 HIPAA Breach Stats: Where Are We At?" HIPAA One blog, August 3, 2017. http://www.hipaaone.com/2017-hipaa-breach-stats/.
3. "Melamedia's Health Information Privacy/Security Alert." Press release, July 25, 2017. http://www.healthcareupdatenewsservice.com/blasts/2017/Melamedia20170725.html.
4. Ponemon Institute. "2016 Ponemon Annual Benchmark Study on Patient Privacy and Data Security." May 2016. https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf.
5. HHS.gov. "Fact Sheet: Ransomware and HIPAA." https://www.hhs.gov/sites/default/files/Ransomware-FactSheet.pdf?language=es.
6. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules," p. 5695.
7. "Fact Sheet: Ransomware and HIPAA."
8. Ibid.
9. Ibid.
10. AHIMA. "Performing a Breach Risk Assessment." *Journal of AHIMA* 84, no. 9 (September 2013): 66-70. http://library.ahima.org/doc?oid=107071.
11. Department of Health and Human Services. "HIPAA Administrative Simplification Regulation Text (Unofficial Version, as amended through March 26, 2013)." https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf, pp. 71-72.
12. Ibid.
13. AHIMA. "Template: Health Information Privacy and Security Breach Notification Letter." 2009. http://library.ahima.org/PdfView?oid=98265.
14. "HIPAA Administrative Simplification Regulation Text." Section 164.502(g)(4), p. 80.
15. "HIPAA Administrative Simplification Regulation Text." Section 164.404(a)(2) p. 72.
16. Ibid.
17. "OCR Announces Initiative to Amplify Investigations of Breaches Affecting Fewer than 500 Individuals." Ropes & Gray Health Care Alert, September 1, 2016. https://www.ropesgray.com/en/newsroom/alerts/2016/September/OCR-Announces-Initiative-to-Amplify-Investigations-of-Breaches-Affecting-Fewer-than-500-Individuals.
18. HHS.gov. "Resolution Agreements." https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
19. HHS.gov. "First HIPAA enforcement action for lack of timely breach notification settles for $475,000." January 9, 2017. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/presence/index.html.
20. Office for Civil Rights. "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework." https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.
21. HHS.gov. "Fact Sheet: Ransomware and HIPAA."
22. "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework."

REFERENCES

AHIMA. "Sanction Guidelines for Privacy and Security Violations (2013 update)." *Journal of AHIMA* 84, no.10 (October 2013): expanded web version. http://library.ahima.org/PB/SanctionGuidelines.

Cotter, Paula. "Amendments to Health Privacy Law Grant States Enforcement Powers." National Association of Attorneys General, *NAAGazette* vol. 3, no. 2. http://www.naag.org/publications/naagazette/volume-3-number-2/amendments-to-health-privacy-law-grant-states-enforcement-powers.php.

Department of Health and Human Services. "Guidance on Risk Analysis Requirements under the HIPAA Security Rule." July 14, 2010. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

Department of Health and Human Services. Privacy Complaint Form Package. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf.

Department of Health and Human Services, Office for Civil Rights. "State Attorneys General." http://www.hhs.gov/ocr/ privacy/hipaa/enforcement/sag/index.html.

Greene, Adam. "Time to Take the Training Wheels Off—Adjusting to New HIPAA Challenges." Presentation at HIPAA Collaborative of Wisconsin 2013 Fall Conference, October 18, 2013.

Lee, Johann, Stacy Clark, and John Hickman. "Life's a Breach, Part II: Omnibus Rule Revises What Constitutes a Breach under the HIPAA/HITECH Breach Notification Requirements." Alston & Bird LLP, May 8, 2013. http://www.alston.com/ Files/Publication/2f74e6ac-abac-4cfc-8a7c-a5f6950d825f/Presentation/PublicationAttachment/a33a888a-fcea-4ba0-a9f8- ae1466d2242a/Lifes-a-breach.pdf.

McGuire Woods. "Omnibus Final Rule Implements Tiered Penalty Structure for HIPAA Violations." February 14, 2013. https://www.mcguirewoods.com/Client-Resources/Alerts/2013/2/HIPAA-Omnibus-Final-Rule-Implements-Tiered-Penalty-Structure-HIPAA-Violations.aspx.

National Institute of Standards and Technology. "Guide for Conducting Risk Assessments: Information Security." Special Publication 800–30, September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

Pollack, Doug. "Four Risk Factors to Understand Since HIPAA Final Rule on Privacy and Security." *Government Health IT*, February 6, 2013. http://www.healthcareitnews.com/news/4-risk-factors-understand-hipaa-final-rule.

Williamson, Jonell B. "Conducting an Internal Investigation and Making a Voluntary Disclosure." March 27, 2008. http://www.lexology.com/library/detail.aspx?g=f7ea5395-ced9-4fd1-9d32-86f43295f777.

APPENDIX A

GLOSSARY OF TERMS

(Unless otherwise noted, terms are adapted from the AHIMA *Pocket Glossary of Health Information Management and Technology*, fifth edition. Chicago, IL: AHIMA Press, 2017.)

The American Recovery and Reinvestment Act (ARRA): The purpose of this act includes the following: (1) To preserve and create jobs and promote economic recovery. (2) To assist those most impacted by the recession. (3) To provide investments needed to increase economic efficiency by spurring technological advances in science and health. (4) To invest in transportation, environmental protection, and other infrastructure that will provide long-term economic benefits. (5) To stabilize state and local government budgets, in order to minimize and avoid reductions in essential services and counterproductive state and local tax increases (ARRA 2009)

Anti-Virus Software: A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents

[Strong] Authentication: (1) The process of identifying the source of health record entries by attaching a handwritten signature, the author's initials, or an electronic signature (2) Proof of authorship that ensures, as much as possible, that log-ins and messages from a user originate from an authorized source (3) As amended by HITECH, means the corroboration that a person is the one claimed (45 CFR 164.304 2013)

Biometrics: The physical characteristics of users (such as fingerprints, voiceprints, retinal scans, iris traits) that systems store and use to authenticate identity before allowing the user access to a system

Breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part that compromises the security or privacy of the protected health information (45 CFR 164.402 2013)

Breach Risk Assessment: Upon receipt of a reported incident [potential violation], an evaluation and analysis that focuses on the probability that the PHI has been compromised using a combination of factors as identified in the final Omnibus Rule

Break the Glass: Similar to breaking the glass to pull a fire alarm, a type of EHR functionality that adds an extra security step and special protections for access to a health record [generally for emergency purposes]. A user must "break the glass" usually by re-entering their password and specifying purpose for access. Access is temporary and all actions may be audited

Burden of Proof: A covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at 164.402 (45 CFR 164.414 2009)

Business Associate (BA): As amended by HITECH, with respect to a covered entity, a person who creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services (45 CFR 160.103 2013)

Business Associate Agreement (BAA): As amended by HITECH, a contract between the covered entity and a business associate must establish the permitted and required uses and disclosures of PHI by the business associate and provides specific content requirements of the agreement. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of HIPAA, and requires termination of the contract if the covered entity or business associate are aware of noncompliant activities of the other (45 CFR 164.504 2013)

Covered Entity (CE): As amended by HITECH, (1) a health plan, (2) a healthcare clearinghouse, (3) a healthcare provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter (45 CFR 160.103 2013)

Criminal Investigation: Criminal investigation is an applied science that involves the study of facts, used to identify, locate, and prove the guilt of a criminal[1]

Dashboards: Reports of process measures to help leaders follow progress to assist with strategic planning; also called scorecards

Department of Health and Human Services (HHS): The cabinet-level federal agency and principal agency for protecting the health of all Americans and providing essential human services, especially for those who are at least able to help themselves (HHS 2013)

Encrypted Wireless: A wireless network on which messages are encrypted (e.g., using Wi-Fi Protected Access 2 (WPA2), Wireless Application Protocol (WAP), Wireless Transport Layer Security Protocol (WTLS), or other appropriate algorithms) to prevent reading by unauthorized parties[2]

Electronic Protected Health Information (ePHI): Information transmitted by electronic media, and information maintained in electronic media

Electronic Prescribing (e-Prescribing/e-Rx): When a prescription is written from the personal digital assistant and an electronic fax or an actual electronic data interchange transaction is generated that transmits the prescription directly to the retail pharmacy's information system

Firewall: A computer system or a combination of systems that provides a security barrier or supports an access control policy between two networks or between a network and any other traffic outside the network

Fraud Alert: Under the Fair and Accurate Credit Transactions Act of 2003 (FACT), requires that consumer reporting agencies, upon the request of a consumer who believes he is or about to be a victim of fraud or any other related crime, must place a fraud alert on that consumer's file for at least 90 days, and notify all other consumer reporting agencies of the fraud alert[3]

Health Information Exchange Organizations (HIEs): An organization that supports, oversees, or governs the exchange of health-related information among organizations acceding to nationally recognized standards[4]

Health Information Technology for Economic and Clinical Health Act (HITECH): Legislation created to promote the adoption and meaningful use of health information technology in the United States. Subtitle D of the Act provides for additional privacy and security requirements that will develop and support electronic health information, facilitate information exchange, and strengthen monetary penalties. Signed into law on February 17, 2009, as part of ARRA (Public Law 111-5 2009)

Health Insurance Portability and Accountability Act of 1996 (HIPAA): The federal legislation enacted to provide continuity of health coverage, control fraud and abuse in healthcare, reduce healthcare costs, and guarantee the security and privacy of health information; limits exclusion for pre-existing medical conditions, prohibits discrimination against employees and dependents based on health status, guarantees availability of health insurance to small employers, and guarantees renewability of insurance to all employees regardless of size; requires covered entities (most healthcare providers and organizations) to transmit healthcare claims in a specific format and to develop, implement, and comply with the standards of the Privacy Rule and the Security Rule; and mandates that covered entities apply for and utilize national identifiers in HIPAA transactions (Public Law 104-191 1996); also called the Kassebaum-Kennedy Law

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

Intrusion Detection System (IDS): Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations)[5]

Logical Access Control: Tools used for identification, authentication, authorization, and accountability in computer information systems. They are components that enforce access control measures for systems, programs, processes, and information. Logical access controls can be embedded within operating systems, applications, add-on security packages, or database and telecommunication management systems[6]

Mitigate/Mitigation: The privacy rule requires covered entities to lessen, as much as possible, harmful effects that result from the wrongful use and disclosure of protected health information. Possible courses of action may include an apology; disciplinary action (also called sanctions) against the responsible employee or employees (although such results will not be able to be shared with the wronged individual); repair of the process that resulted in the breach; payment of a bill or financial loss that resulted from the infraction; or gestures of goodwill and good public relations, such as a gift certificate, that may assuage the individual (45 CFR 164.530 2009)

Office for Civil Rights (OCR): Department in HHS responsible for enforcing civil rights laws that prohibit discrimination on the basis of race, color, national origin, disability, age, sex, and religion by healthcare and human services entities over which OCR has jurisdiction, such as state and local social and health services agencies, and hospitals, clinics, nursing homes, or other entities receiving federal financial assistance from HHS. This office also has the authority to ensure and enforce the HIPAA Privacy and Security Rules; Responsible for investigating all alleged violations of the Privacy and Security Rules (OCR 2013)

Packet Filtering (also known as Sniffers): A software security product that runs in the background of a network, examining and logging packet traffic and serving as an early warning device against hackers

Personal Health Record (PHR): An electronic or paper health record maintained and updated by an individual for himself or herself; a tool that individuals can use to collect, track, and share past and current information about their health or the health of someone in their care

Physical Security (Physical Safeguards): As amended by HITECH, security rule measures such as locking doors to safeguard data and various media from unauthorized access and exposures; including facility access controls, workstation use, workstation security, and device and media controls (45 CFR 164.310 2013)

Protected Health Information (PHI): As amended by HITECH, individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years (45 CFR 160.103 2013)

Ransomware: a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates2 data, or ransomware in conjunction with other malware that does so[7]

Reasonable Cause: As amended by HITECH, an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associated did not act with willful neglect (45 CFR 160.401 2013)

Reasonable Diligence: As amended by HITECH, means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances (45 CFR 160.401 2013)

Sanctions: Penalties or other methods of enforcement used to provide incentives for compliance with laws or rules and regulations such as the HIPAA Privacy and Security Rules and related policies and procedures of the covered entity; sanctions should be uniform across organizations (45 CFR 164.308 2013)

Scorecards: Reports of outcomes measures to help leaders know what they have accomplished; also called dashboards

Subcontractors: As amended by HITECH, a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate (45 CFR 160.103 2013)

Unsecured Protected Health Information: As amended by HITECH, protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the secretary in the guidance issued under section 13402(h)(2) of Public Law 111-05 (45 CFR 164.402 2013)

Violation [of the HIPAA Privacy and or Security Rule]: occurs in those instances where unsecured PHI was acquired, used or disclosed in a manner not permitted by the rules

Very Important Person (VIP) Record: A designation given to records of individuals which may be accessed by users out of curiosity. VIPs are generally celebrities, sports figures, public figures, or patients with unusual conditions or circumstances

Willful Neglect: As amended by HITECH, conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated (45 CFR 160.401 2013)

Notes

1. "Criminal Investigation." http://en.wikipedia.org/wiki/Criminal_investigation.

2. National Institute of Standards and Technology. "Glossary of Key Information Security Terms."

3. "Fair and Accurate Credit Transactions Act." http://en.wikipedia.org/wiki/Fair_and_Accurate_Credit_Transactions_Act#Fraud_alerts.

4. Department of Health and Human Services. "The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Terms." 2008.

5. National Institute of Standards and Technology. "Glossary of Key Information Security Terms."

6. "Logical Access Control." http://en.wikipedia.org/wiki/Logical_access_control.

7. National Institute of Standards and Technology. "Glossary of Key Information Security Terms."

APPENDIX B

HIPAA BREACH NOTIFICATION CHECKLIST

Case #: _____

Tracking Deadlines

_____ Date of receipt of reported incident

_____ Date breach occurred

_____ Date breach discovered

_____ Deadline for notifications (30/60 days post-discovery)

_____ If applicable, law enforcement determination of notification delay (based on hindering criminal investigation or causing damage to national security): If so,

___ Documentation of determination

___ Extended deadline for notifications: _____

Process Steps

___ Internal investigation (summary of event and conclusions)

___ Breach risk assessment performed; OR

___ Immediate determination that breach has occurred—no risk assessment necessary

___ Review of state breach laws

Business Associate (if applicable)

___ Current Business Associate Agreement

___ Met the terms of the BAA breach notification section

___ Other: _____

Notification of Breach

___ Internal Senior Leadership/Legal Department

___ Patient

Letter includes the following:

1. Brief description of what happened
   a. Includes date of the breach
   b. Includes date of discovery
2. Description of the type of unsecured PHI involved
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach
4. Brief description of what the CE involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
5. Contact procedures to ask questions, which must include a toll-free number, an e-mail address, website, or postal address

The following items may be included in a breach notification letter:

1. Recommendations that the individual contact their credit card company, and how to contact credit bureaus and obtain credit monitoring services
2. Information about the steps the CE is taking to retrieve the breached information (such as filing a police report)
3. Information about steps the CE is taking to improve security to prevent future similar breaches

___ FAQ talking points for contact person

___ Annual DHHS Report

>500 Patients

___ Secretary of HHS (Date: _____)

___ Local News Media (____Newspaper ____Press Release ____ Other)

___ Substitute Notice (__Yes or __No)

Mitigation

___ Assurances received

___ Patient notified of breach within 30 days of discovery

___ Recovery/destruction of PHI

___ Identity theft protection

___ Change in policy/procedures

___ Implement additional safeguards

___ Other: _____

Education and Training

__ Education and Training: _____ _____
_____

__ Education and Training: _____ _____
_____

__ Education and Training: _____ _____
_____

Sanctions

___ Level 1 ___ Level II ___ Level III ___ Level IV

___ Other: _____

APPENDIX C

(Source: "Performing a Breach Risk Assessment," Journal of AHIMA 84, no. 9 (Sept. 2013): 66-70.)

SAMPLE BREACH RISK ASSESSMENT SCORING MATRIX

The Department of Health and Human Services provides a number of resources that assist in completing an appropriate risk assessment under the Security Rule. These guidelines may be used as a method for scoring the probability of a breach under the provisions of the Breach Notification Rule. There are many scoring methodologies that could be utilized to quantitatively assist in determining the low probability of compromise. This model is one that may be used as a scoring tool to assist in the organization's decision making.

Evaluating each of the four factors utilizing this type of tool provides an objective assessment of the probability that PHI, impermissibly used or disclosed, has been compromised. The four factors should be reviewed and analyzed as a whole. Each factor may show an increased or decreased probability that the PHI was compromised.

How to Use the Matrix:

Each risk factor is assessed based on the evaluation questions provided below. A score is determined based on the likelihood that the information has been compromised, multiplied by the potential impact that the PHI could be compromised. If any factor is scored greater than 10 (Minimal or Low) the probability of compromise is moderate to severe suggesting appropriate breach notification. However, it is important to keep in mind that a score of 10 in one factor can balance out when evaluated in combination with another factor(s). In other words, one factor when considered in combination with another can lead to different results. Each incident is different and must be treated as such.

SCORING MATRIX

Likelihood*	**Impact****		
	Minimal 10	**Moderate** 50	**Severe** 100
High 1.0	Minimal 10	Medium 50	High 100
Medium 0.5	Minimal 5	Medium 25	Medium 50
Low 0.1	Minimal 1	Low 5	Low 10

*Likelihood

- **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*

**Impact

- **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.*

Risk Factors	*Evaluation Questions*	*Factor Evaluation/ Mitigation Strategy*	*Likelihood*	*Impact*	*Score (Score = Likelihood x Impact)*
Nature and Extent of PHI Involved:	The goal of evaluating this factor is to determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipients own interests.				
	Which patient identifiers were used or disclosed? Does the combination of identifiers used or disclosed increase risk? Are there particular identifiers such as a Social Security Number (SSN) that raise concerns?				
	Does the PHI used or disclosed contain a sensitive diagnosis? (e.g. substance abuse, mental health, sexually transmitted disease (STD), HIV, cancer)				
	Does the amount of PHI used or disclosed increase the risk?				
	Does the use or disclosure reveal the PHI of a well-known individual?				
	Does the PHI used or disclosed include sufficient indirect patient identifiers that re-identification of individuals is possible?				
Unauthorized Person to whom disclosure was made:	The goal of evaluating this factor is to determine the probability as to whether the recipient might further use or disclose the PHI in a manner adverse to the individual or for the recipient's own interests.				
	Does the unauthorized recipient have obligations to protect the privacy and security of the disclosed information such as a BA or another CE?				
	Is the recipient a member of your internal workforce or a Business Associate such that you can ensure that the PHI will not be further used or disclosed?				
	Does the recipient have a relationship with the individual where they are likely to act in the individual's best interest?				
	Is there additional risk if the recipient likely knows the subject of the PHI?				
	If the recipient impermissibly used the PHI what was their purpose or motive for doing so? •Unintentional or inadvertent error? •Intentional for self-serving, malicious, or harmful reasons?				

Risk Factors	*Evaluation Questions*	*Factor Evaluation/ Mitigation Strategy*	*Likelihood*	*Impact*	*Score (Score = Likelihood x Impact)*
	What was the attitude and demeanor of the unauthorized recipient? Were they co-operative and willing to work with you to secure the PHI? Were they also concerned about protecting the PHI? Did they initiate contact with you right away or did they appear reluctant to cooperate as leverage for something else they wanted for their own best interests?				
	Was the recipient an unintended recipient or did they seek out the information?				
	If only indirect identifiers were disclosed, does the recipient have the ability to re-identify the PHI?				
	Is it believed that the PHI was taken with intent to use or sell?				
The actual use of the PHI disclosed:	The goal of evaluating this factor is to determine whether or not the PHI was actually acquired or viewed or whether there was an opportunity for the PHI to be acquired or viewed. The probability of compromise is lower only if the opportunity existed for the PHI to be acquired or viewed but the PHI was not actually acquired or viewed.				
	Was the PHI actually acquired or viewed by an unauthorized person?				
	Is it possible to demonstrate that the disclosed PHI was never accessed, viewed, or acquired?				
	If an electronic device is involved, does forensic analysis show that the PHI was accessed, acquired, viewed, transferred, or compromised?				
	If ePHI is involved, what does the audit trail indicate? What actions (e.g., print, view) were taken? What parts of the record were accessed?				
The extent to which the risk to the PHI was mitigated:	The goal in evaluating this factor is to determine how thoroughly and quickly the PHI involved has been secured following the impermissible use or disclosure.				
	If the recipient was a CE or other reliable business otherwise bound by privacy obligations (e.g., BAs, banks or attorneys), was verbal confirmation given and documented that PHI was destroyed?				

Risk Factors	*Evaluation Questions*	*Factor Evaluation/ Mitigation Strategy*	*Likelihood*	*Impact*	*Score (Score = Likelihood x Impact)*
	If the recipient was not a CE or other reliable business otherwise bound by privacy obligations, was written confirmation of destruction obtained?				
	If the recipient was an employee who impermissibly used PHI, was a statement of assurance obtained attesting that PHI will not be further used or disclosed?				
	Has satisfactory assurance been obtained from the unauthorized recipient that the disclosed PHI will not be further used or disclosed or will be destroyed? Has an effective mitigation strategy been implemented such that further unauthorized disclosures are extremely unlikely?				
	Was the PHI returned in a timely manner and intact?				
Overall Assessment	*Note: If any factor is scored greater than 10 (Minimal or Low) the probability of compromise is moderate to severe suggesting appropriate breach notification.*				

NOTE: Each incident will vary based on scenario and organizational policy and procedure. Therefore, each incident should be evaluated independently for probability of compromise. This tool may be used to help provide guidance in assessing risk factors and can be adapted to fit individual need.

APPENDIX D

(Source: "Performing a Breach Risk Assessment," Journal of AHIMA 84, no. 9 (Sept. 2013): 66-70.)

SAMPLE CASE: DETERMINING LOW PROBABILITY OF COMPROMISE

Scenario:

General Hospital faxes a list of surgery patients to an anesthesiologist on a daily basis. The hospital receives a telephone call stating that an attorney's office has been receiving faxes of patient information on a daily basis and believes the information is being sent to the wrong fax number. The incident is reported to the facility privacy officer. Upon further investigation, it is determined that the list of patients contains the name of the hospital, the patient's medical record number, admit date, patient's age, procedure to be performed, and the patient's surgeon. The Privacy Officer contacted the company who reported the breach and it was determined that the fax number was associated with an attorney's office. The secretary, who viewed the information, brought the faxed documents to the attorney's attention. The attorney stated that all the faxed documents were shredded.

How to Use the Matrix:

Each risk factor is assessed based on the evaluation questions provided below. A score is determined based on the likelihood that the information has been compromised multiplied by the potential impact that the PHI could be compromised. If any factor is scored greater than 10 (Minimal or Low) the probability of compromise is moderate to severe suggesting appropriate breach notification. However, it is important to keep in mind that a score of 10 in one factor can balance out when evaluated in combination with another factor(s). In other words, one factor when considered in combination with another can lead to different results. Each incident is different and must be treated as such.

SCORING MATRIX

Likelihood*	**Impact****		
	Minimal 10	**Moderate** 50	**Severe** 100
High 1.0	Minimal 10	Medium 50	High 100
Medium 0.5	Minimal 5	Medium 25	Medium 50
Low 0.1	Minimal 1	Low 5	Low 10

*Likelihood

- **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*

**Impact

- **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.*

Risk Factors	*Evaluation Questions*	*Factor Evaluation/ Mitigation Strategy*	*Likelihood*	*Impact*	*Score (Score = Likelihood x Impact)*
Nature and Extent of PHI Involved:	The goal of evaluating this factor is to determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipients own interests.				
	Which patient identifiers were used or disclosed? Does the combination of identifiers used or disclosed increase risk? Are there particular identifiers such as a Social Security Number (SSN) that raise concerns?	The facility name, medical record number, patient's age, procedure, and surgeon poses a moderate impact that the patient may be identified; however, there is a low likelihood of PHI being impermissibly used or disclosed	.1	50	5 (.1x50)
	Does the PHI used or disclosed contain a sensitive diagnosis? (e.g., substance abuse, mental health, sexually transmitted disease (STD), HIV, cancer)	No sensitive information was disclosed	.1	10	1 (.1x10)
	Does the amount of PHI used or disclosed increase the risk?	Small amount of PHI; thus impact minimal	.1	10	1 (.1x10)
	Does the use or disclosure reveal the PHI of a well-known individual?	No well-known individual	.1	10	1 (.1x10)
	Does the PHI used or disclosed include sufficient indirect patient identifiers that re-identification of individuals is possible?	Re-identification is moderate	.1	50	5 (.1x50)
Unauthorized person to whom disclosure was made:	The goal of evaluating this factor is to determine the probability that the recipient of the protected health information will further use or disclose the PHI in a manner adverse to the individual or for their own interests.				
	Does the unauthorized recipient have obligations to protect the privacy and security of the disclosed information such as a BA or another CE?	No Not a covered entity or business associate			
	Is the recipient a member of your internal workforce or a Business Associate such that you can assure that the PHI will not be further used or disclosed?	N/A			
	Does the recipient have a relationship with the individual where they are likely to act in the individual's best interest?	N/A			

Risk Factors	*Evaluation Questions*	*Factor Evaluation/ Mitigation Strategy*	*Likelihood*	*Impact*	*Score (Score = Likelihood x Impact)*
	Is there additional risk if the recipient likely knows the subject of the PHI?	There is additional risk; however, the attorney provided satisfactory assurances that the information will not be used or disclosed	.1	50	5 (.1x50)
	If the recipient impermissibly used the PHI what was their purpose or motive for doing so? • Unintentional or inadvertent error? • Intentional for self-serving, malicious or harmful reasons?	No impermissible use or disclosure	.1	10	1 (.1x10)
	What was the attitude and demeanor of the unauthorized recipient? Were they cooperative and willing to work with you to secure the PHI? Were they also concerned about protecting the PHI? Did they initiate contact with you right away or did they appear reluctant to cooperate as leverage for something else they wanted for their own best interests?	The likelihood of the unauthorized person re-disclosing the information is low. Satisfactory assurances were given in good faith by shredding the documents. The probability of improper use or disclosure is minimal; therefore, the impact is also minimal	.1	10	1 (.1x10)
	Was the recipient an unintended recipient or did they seek out the information?	Information not sought	.1	10	1 (.1x10)
	If only indirect identifiers were disclosed, does the recipient have the ability to re-identify the PHI?	Most were direct identifiers	.1	50	5 (.1x50)
	Is it believed that the PHI was taken with intent to use or sell?	No intent to use or sell PHI	.1	10	1 (.1x10)
The use of the disclosure:	The goal of evaluating this factor is to determine whether or not the PHI was actually acquired or viewed or whether there was an opportunity for the PHI to be acquired or viewed. The probability of compromise is lower if only the opportunity existed for the PHI to be acquired or viewed but the PHI was not actually acquired or viewed.				
	Was the PHI actually acquired or viewed by an unauthorized person?	Information was acquired and viewed; however the likelihood of re-disclosure is low	.1	100	10 (.1x100)

Risk Factors	*Evaluation Questions*	*Factor Evaluation/ Mitigation Strategy*	*Likelihood*	*Impact*	*Score (Score = Likelihood x Impact)*
	Is it possible to demonstrate that the disclosed PHI was never accessed, viewed, or acquired?	N/A It was determined that PHI was accessed and viewed; therefore, this factor is not applicable			
	If an electronic device is involved, does forensic analysis show that the PHI was accessed, acquired, viewed, transferred or compromised?	N/A No forensic analysis completed. Reason may or may not be documented.			
	If ePHI is involved, what does the audit trail indicate? What actions (e.g., print, view) were taken? What parts of the record were accessed?	N/A			
The extent to which the risk to the PHI was mitigated:	The goal in evaluating this factor is to determine how thoroughly and quickly the PHI involved has been secured following the impermissible use or disclosure.				
	If the recipient was a CE or other reliable business otherwise bound by privacy obligations (e.g., BAs, banks or attorneys), was verbal confirmation given and documented that PHI was destroyed?	Verbal and written confirmation was given that the PHI was destroyed	.1	10	1 (.1x10)
	If the recipient was not a CE or other reliable business otherwise bound by privacy obligations, was written confirmation of destruction obtained?	N/A			
	If the recipient was an employee who impermissibly used PHI, was a statement of assurance obtained attesting that PHI will not be further used or disclosed?	N/A			
	Has satisfactory assurance been obtained from the unauthorized recipient that the disclosed PHI will not be further used or disclosed or will be destroyed? Has an effective mitigation strategy been implemented such that further unauthorized disclosures are extremely unlikely?	Satisfactory assurances have been obtained that the PHI will not be further used or disclosed. Mitigation strategies were put into place (see overall assessment)			

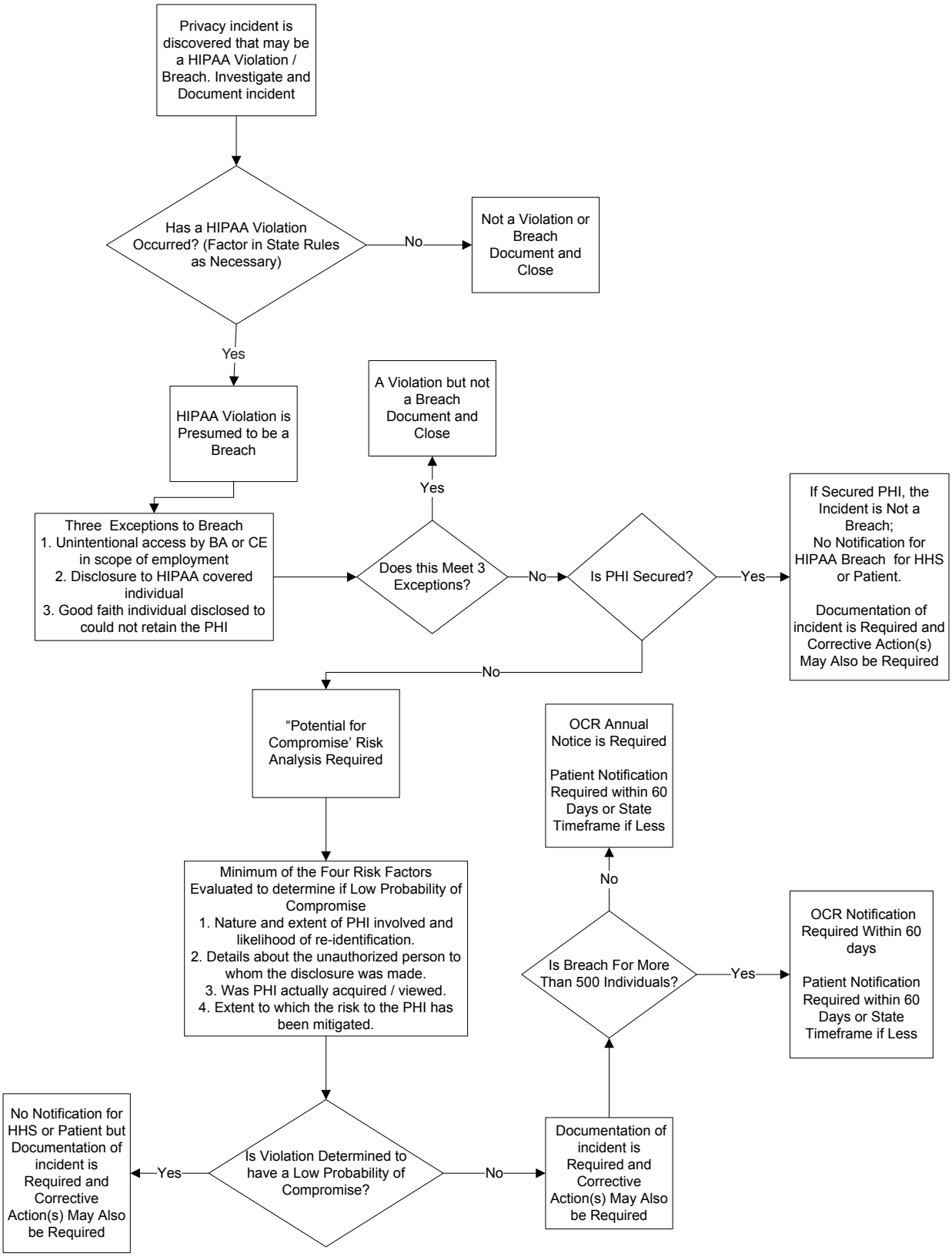
Risk Factors	*Evaluation Questions*	*Factor Evaluation/ Mitigation Strategy*	*Likelihood*	*Impact*	*Score (Score = Likelihood x Impact)*
	Was the PHI returned in a timely manner and intact?	PHI was destroyed	.1	10	1 (.1x10)
Overall Assessment and Mitigation Strategy	*Note: If any factor is scored greater than 10 (Minimal or Low) the probability of compromise is moderate to severe suggesting appropriate breach notification.* *The Privacy Officer of General Hospital worked closely with the attorney to explain the accidental disclosure, identify the appropriate fax number from the anesthesiologist and obtained satisfactory assurances that the information would not be re-disclosed.* ***Upon scoring of each of the risk assessment factors, none of the scores assessed was greater than 10 and therefore, no reporting is necessary. The determination of the scoring within this risk assessment identifies that there is a low probability that protected health information has been compromised.*** *The incident was thoroughly researched and the fax number of the anesthesiologist was corrected. The anesthesiologist was queried to determine the minimum necessary PHI and the report was modified accordingly.*				

***NOTE**: Each incident will vary based on scenario and organizational policy and procedure. Therefore, each incident should be evaluated independently for probability of compromise. This tool may be used to help provide guidance in assessing risk factors and can be adapted to fit individual need.*

APPENDIX E

(Source: "Performing a Breach Risk Assessment," Journal of AHIMA 84, no. 9 (Sept. 2013): 66-70.)

SAMPLE BREACH DECISION TREE



APPENDIX F

(Source: "Draft Template: Health Information Privacy and Security Breach Notification Letter." 2009. Library.ahima.org/Pdfview?oid=98265.)

SAMPLE BREACH NOTIFICATION LETTER

Letterhead Recommended
(Includes organization's full name and address)

[Date]

[Victim or Representative Name]
[Address Line 1]
[Address Line 2]
[City, State Zip Code]

Re: Personal *[Health]* Information of *[Name of Victim]*

Dear [Addressee Name—Victim or Representative]:

On *[date], [name of responsible healthcare organization]* became aware of a breach of *[your/loved one's]* personal health information. We *[have identified/estimate]* the date of information leakage to be *[date]. OR [The duration of information exposure was (include date range and time range)].* OR [*We are unable to determine the date of the breach occurrence.]* We are notifying affected individuals in as timely a manner as possible so you can take swift personal action along with our organization's efforts to reduce or eliminate potential harm. *[It was necessary to delay notification because of the protected nature of the forensic investigation.]* Incident investigation *[is/is not]* complete at this time.

The incident involving protected health information was *[loss/theft/other] [state the circumstances]. [Examples: theft of a laptop containing files of 5,326 individuals from the trunk of a car* OR *exposure of personal health information on the (name of organization) Web site* OR *misplacement of five boxes, 250 paper medical records, during transit to a vendor destruction site].* The unsecured information includes *[list the types of information involved: part/complete medical records dated between (state date range), full name, Social Security Number, date of birth, home address, account number, diagnosis, types of treatment information, disability code, name other information types].*

We recommend immediate steps be taken to protect *[yourself/your loved one]* from *[additional/potential]* information breach harm *[List fitting recommendations such as:]*

- Register a fraud alert with the three credit bureaus listed here; and order credit reports:
  - » Experian: (888) 397-3742; www.experian.com; PO Box 9532, Allen, TX 75013
  - » TransUnion: (800) 680-7289; www.transunion.com; Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790
  - » Equifax: (800)525-6285; http://www.equifax.com; PO 740241, Atlanta, GA 30374-0241
- Monitor account statements, EOBs, and credit bureau reports closely
- Contact the Consumer Protection Agency [Sample Google search for appropriate state: "consumer protection agency Illinois"]
- (If the consumer has validation their information has been compromised) Notify law enforcement to assist the investigation: [Provide advice on how to file and provide contact information for local law enforcement, the state attorney general office, and the Federal Trade Commission]
- Access helpful Web links to learn additional information on consumer protection when personal information is compromised. [List Web links or provide own organization's Web site] [For example, include AHIMA's Medical Identity Theft Response Checklist for Consumers: *http://library.ahima.org/Pdfview?oid=82205*

[Name of responsible healthcare organization/s] [has/have taken OR *will soon take]* these steps to protect your, and others', personal information from further harm or similar circumstances: *[Choose from or customize these examples or add your own]:*

- Initiated a forensics security investigation
- Filed a police report on [date]; Initiated a criminal investigation
- Sanctioned five employees/a physician by suspension/termination of employment/medical staff privileges
- Address operational or technology updates or changes triggered by the incident to improve
  - » confidentiality, such as strengthening technology safeguards or administrative policies and/procedures
- List steps a business associate is taking or investigation/cancellation of a business associate contract
- List any specific, relevant state law factors/directives
- Other

State Law Customization Considerations—At appropriate points in the letter above, insert additional information required by state law such as:

- Number of involved victims
- Potential level of threat to victims
- Possible future information security threats victims should be aware of
- The definition of PHI in your state
- What agencies were notified (i.e., state health department, state attorney general, state police)

Furthermore, [name or responsible healthcare organization] is offering (you/name of individual) # years of free credit monitoring service. To take advantage of this offer, (give instructions to initiate the protection)].

[Name of responsible healthcare organization] sincerely apologizes for the inconvenience and concern this incident causes you. Your information privacy is very important to us and we will continue to do everything we can to correct this situation and fortify our operational protections for you and others.

You may contact us with questions and concerns in the following ways: *[by calling our Privacy Office at our toll free number (XXX) XXX-XXXX between the hours of X a.m. and X p.m., 24 hours or Monday to Friday; sending an e-mail message to xxxx@xxxx.org; addressing a letter to our postal address, Anywhere Hospital, 1234 Hospital Way, City, State].*

Sincerely,

[Name and title of an individual with knowledge of the incident]

[Contact information—may be the same as the contact information listed above]

APPENDIX G

SAMPLE NOTICES AND STATEMENTS

Sample Privacy Notice: Incident Involving a Vendor

ABC Health Insurance recently learned of a situation in which an employee at DEF Vendor, a call-center vendor, confessed to Social Security Administration (SSA) investigators that she took Social Security numbers, including those from members of ABC Health insurance. There are indications that the employee may have conveyed some of this information to third parties who are the subject of an ongoing federal criminal investigation. This individual's employment with DEF Vendor was terminated immediately upon DEF Vendor becoming aware of the incident.

ABC Health Insurance has worked diligently since discovery of this matter to identify all members whose information may have been impacted by the DEF Vendor's employee. While the investigation is ongoing, four members have been identified as impacted to date. We notified these members to offer them free identity theft protection service. Additionally, other ABC Health Insurance members whose information could have been impacted were also notified about the incident and offered free identity theft protection service. We believe the number of impacted members is much smaller than the number of members we are notifying. The law enforcement agencies have advised us that the list does not currently exceed 300. An investigation into the incident is underway at various law enforcement agencies. Both ABC Health Insurance and DEF Vendor are fully cooperating with the investigation. We were unable to locate certain potentially affected individuals and are providing this notice on our website to notify those individuals of this event. Should you have any questions about this notice, you may call us at 1 (555) 555-5555.

Sample Substitute Notice

NOTICE OF POSSIBLE UNAUTHORIZED RELEASE OF MEDICAL RECORDS: Between 2005 and 2010 ABC Hospital released a number of patient records to third parties in compliance with subpoenas that may not have met legal requirements of federal privacy laws. We do not have current contact information on some of our past patients whose records were released. Any of our prior patients may contact Jane Doe, HIM Director, at (555) 555-5555 to determine whether your records were released.

Sample Media Statement

A few weeks ago, ABC Hospital discovered and reported a burglary and theft of a computer from a locked office in the hospital's off-site imaging center. The imaging center operates in a remote location approximately three miles from the hospital. The police were immediately notified and the case is currently under investigation.

The computer that was stolen was last used in 2008 and contained password protected data including clinical information, patient billing information and some employee records from the hospital. The data contained the names, social security numbers, addresses, and diagnostic information on 3,500 patients who were treated prior to 2008. The number of records stored on this equipment represents less than .5 percent of the total number of former patients in the hospital's database.

The hospital has not received any reports of identity theft or misuse of information as a result of this incident. However, the hospital is offering patients complimentary participation in an identity theft protection program. Each patient has received, or will receive in a few days, a letter notifying them of the burglary and a phone number they can call with additional questions.

We sincerely regret this incident and any inconvenience this may cause our patients whose privacy we take very seriously. We are in the process of implementing new measures to ensure the safest data security possible. These measures include reviewing security policies and procedures at all remote locations, pursuing enhanced data security encryption and engaging a third party security company to assist in refining our data security program.

APPENDIX H

(Source: Department of HHS, "Instructions for Submitting Notice of a Breach to the Secretary." www.hhs.gov.)

HHS BREACH REPORTING WORKSHEET

Breach Affecting:

- 500 or more individuals
- Less than 500 individuals

Report Type:

- Initial Breach Report
- Addendum to Previous Report

SECTION 1—COVERED ENTITY:

Name of Covered Entity:_____

Address: _____

City:_____ State: _____ Zip Code: _____

Contact Name _____

Contact Phone Number: (XXX) XXX-XXXX _____

Contact E-mail: _____

Type of Covered Entity: _____

SECTION 2—BUSINESS ASSOCIATE

Name of Business Associate: _____

Address: _____

City:_____ State: _____ Zip Code: _____

Contact Name: _____

Contact Phone Number: (XXX) XXX-XXXX _____

Contact E-mail: _____

SECTION 3—BREACH

Date(s) of Breach: ____/___/____ - ____/___/____

MM/DD/YYYY – MM/DD/YYYY

Date(s) of Discovery: ____/___/____ - ____/___/____

MM/DD/YYYY–MM/DD/YYYY

Approximate number of Individuals Affected by the Breach: _____

Breach:

Type of Breach

» Theft

» Loss

» Improper Disposal

» Unauthorized Access/Disclosure

» Hacking/IT Incident

» Unknown

» Other—Describe type of breach: _____

Location of Breached Information:

- Laptop
- Desktop Computer
- Network Server
- E-mail
- Other portable electronic device
- Other (describe in detail location description)

_____

_____

_____

Type of Protected Health Information (PHI) Involved in the Breach:

- Demographic Information
- Financial Information
- Clinical Information
- Other (describe location of breach, how the breach occurred and any additional information regarding the type of breach, type of media, type of PHI involved in the breach)

_____

_____

_____

Brief Description of Breach: _____

Safeguards in Place Prior to Breach: (Protective measures in place prior to the breach)

Refer to appendix A for the definitions of each option listed here.

- *Privacy Rule Safeguards (Training, Policies and Procedures, etc.)*
- *Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)*
- *Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)*
- *Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)*

SECTION 4— NOTICE OF BREACH AND ACTIONS TAKEN

Date(s) Individual Notice Provided: ____/___/____ - (____/___/____)

MM/DD/YYYY (- MM/DD/YYYY)

Was Substitute Notice Required? ❑ Yes ❑ No

Was Media Notice Required? ❑ Yes ❑ No

Actions Taken in Response to Breach: (Provide detailed information for actions taken following the breach in addition to those selected.)

- Security and/or Privacy Safeguards
- Mitigation
- Sanctions
- Policies and Procedures
- Other: _____

_____

SECTION 5—ATTESTATION

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS website pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

Name:_____ Date:_____

Typing your name represents your signature MM/DD/YYYY