Performing a Breach Risk Assessment - Retired

Save to myBoK

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.

Modifications to the 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 were published by HHS on January 25, 2013. This "omnibus" final rule encompasses significant modifications to the interim final rule for breach notification, of which a breach risk assessment remains an essential component. Although the final rule became effective on March 26, 2013, covered entities (CEs) and business associates (BAs) have until September 23, 2013 to meet compliance.

This practice brief is intended to provide guidance for performing a thorough risk assessment to determine the level of probability that the PHI in question was compromised.

The Final Rule: Breach Requirements

The omnibus final rule modifies and clarifies the definition of a breach and risk assessment approach that was outlined in the interim final rule. As outlined in the interim final rule, a "breach" is defined as "the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information." For further details on the breach definition outlined in the interim final rule, see the sidebar on below.

Interim Final Rule Outlines Breach Definition

The definition of a breach outlined in the interim final rule includes three exceptions:

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 CE 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.

Source: Department of Health and Human Services. "Notification in the Case of Breach of Unsecured Protected Health Information." *Federal Register*. 45 CFR 164.402. October 1, 2011.

The final rule added language to the definition of a breach to clarify that an impermissible use or disclosure of PHI is presumed to be a breach, and therefore requires notification to the individual. There is an exception to this circumstance if the covered entity's business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. This new language is also consistent with the administrative requirements and burden of proof stipulations, which provide that covered entities and business associates have the burden of proof to demonstrate that all notifications were

made as required or that an impermissible use or disclosure did not constitute a breach as defined. The covered entity or BA must maintain sufficient documentation to meet the needs of burden of proof.[2] To ensure that this provision is applied uniformly and objectively by covered entities and business associates, the final rule removed the harm standard and modified the risk assessment to focus more objectively on the probability that the PHI has been compromised using a combination of determination factors, identified in the rule, that are more objective than the previous harm threshold standard.

It should be noted that the final rule interprets the terms "acquisition" and "access" as elements of the current definitions of "use" and "disclosure" as defined by the HIPAA rules. For example, an acquisition may be a "use" or "disclosure" depending on who acquired the information (i.e., a workforce member or someone outside the CE, such as a business associate).[3]

Determining the Presence of a PHI Violation

The interim final rule defines unsecured PHI as information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the HHS Secretary in the guidance issued under section §13402(h)(2) of the American Recovery and Reinvestment Act. The guidance specifies that only encryption and destruction consistent with the National Institute of Standards and Technology (NIST) guidelines renders PHI unusable, unreadable, or indecipherable.

These guidelines, if used, create the functional equivalent of a safe harbor and notification is not required in the event of a breach. The guidance may be used to render PHI unusable, unreadable, and indecipherable to unauthorized persons, and is published on the HHS website. If PHI has not been secured in accordance with the specified guidance and a violation has occurred, then it must be presumed to be a breach.

It is important to review the workflow for the investigation of a privacy or security incident prior to conducting a risk assessment. The process starts with the discovery of a potential violation of the HIPAA Privacy Rule. 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 rules. If the PHI was acquired, accessed, used, or disclosed in a manner not permitted by the rule, a violation has occurred.

The final rule now requires that the entity must presume the violation to be a breach unless one of the three exceptions applies. At that point, the entity must move forward with the risk assessment to demonstrate if the probability is low that the PHI has been compromised or else provide notification to the affected individual or individuals. The preamble of the final rule states that a covered entity or business associate has the discretion to provide the required notification following an impermissible use or disclosure of PHI without performing a risk assessment. Because the final rule clarifies that the presumption should be made that a breach has occurred following every impermissible use or disclosure of PHI, entities may decide to notify without conducting a risk assessment that evaluates the probability PHI has been compromised.

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 (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 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 CE, 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 BA or another CE?
- Is the recipient a member of your internal workforce or a BA such that you can assure 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 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 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 electronic PHI (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

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 utilized. 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 and defined as follows:

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

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

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

Document to Meet Burden of Proof

The covered entity or business associate bears the burden of proof to demonstrate that all notifications were made as required or that the impermissible use or disclosure did not constitute a breach. 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

If the risk assessment is not completed or if low probability cannot be demonstrated, then documentation of all notifications made must also be maintained to ensure compliance with this requirement. Documentation provides the safeguard for the CE

or BA in the event the determination is called into question.

- See Appendix A for a sample tool that may be utilized to assist in scoring each factor and documenting the risk assessment.
- See Appendix B for a sample case using Appendix A and the scoring table above to help demonstrate low probability of compromise.
- See Appendix C for a decision tree diagram that follows the workflow from the point an incident is reported through the actions necessary for compliance.

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." *Federal Register*. 45 CFR Parts 160 and 164. January 25, 2013. https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the.
2. Ibid.
3. Ibid.

Appendix A: 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?				

Risk Factors	Evaluation Questions	Factor Evaluation/ Mitigation Strategy	Likelihood	Impact	Score (Score = Likelihood x Impact)
	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 assure 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?				
	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?				

Risk Factors	Evaluation Questions	Factor Evaluation/ Mitigation Strategy	Likelihood	Impact	Score (Score = Likelihood x Impact)
	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.				

Risk Factors	Evaluation Questions	Factor Evaluation/ Mitigation Strategy	Likelihood	Impact	Score (Score = Likelihood x Impact)
	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?				
	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 B: 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 ofimproper 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)

Risk Factors	Evaluation Questions	Factor Evaluation/ Mitigation Strategy	Likelihood	Impact	Score (Score = Likelihood x Impact)
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			
	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	No impermissible use or disclosure	.1	10	1 (.1x10)

Risk Factors	Evaluation Questions	Factor Evaluation/ Mitigation Strategy	Likelihood	Impact	Score (Score = Likelihood x Impact)
	or harmful reasons?				
	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.				

Risk Factors	Evaluation Questions	Factor Evaluation/ Mitigation Strategy	Likelihood	Impact	Score (Score = Likelihood x Impact)
	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)
	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)

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?	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)			
	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***				

Risk Factors	Evaluation Questions	Factor Evaluation/ Mitigation Strategy	Likelihood	Impact	Score (Score = Likelihood x Impact)
	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.*				

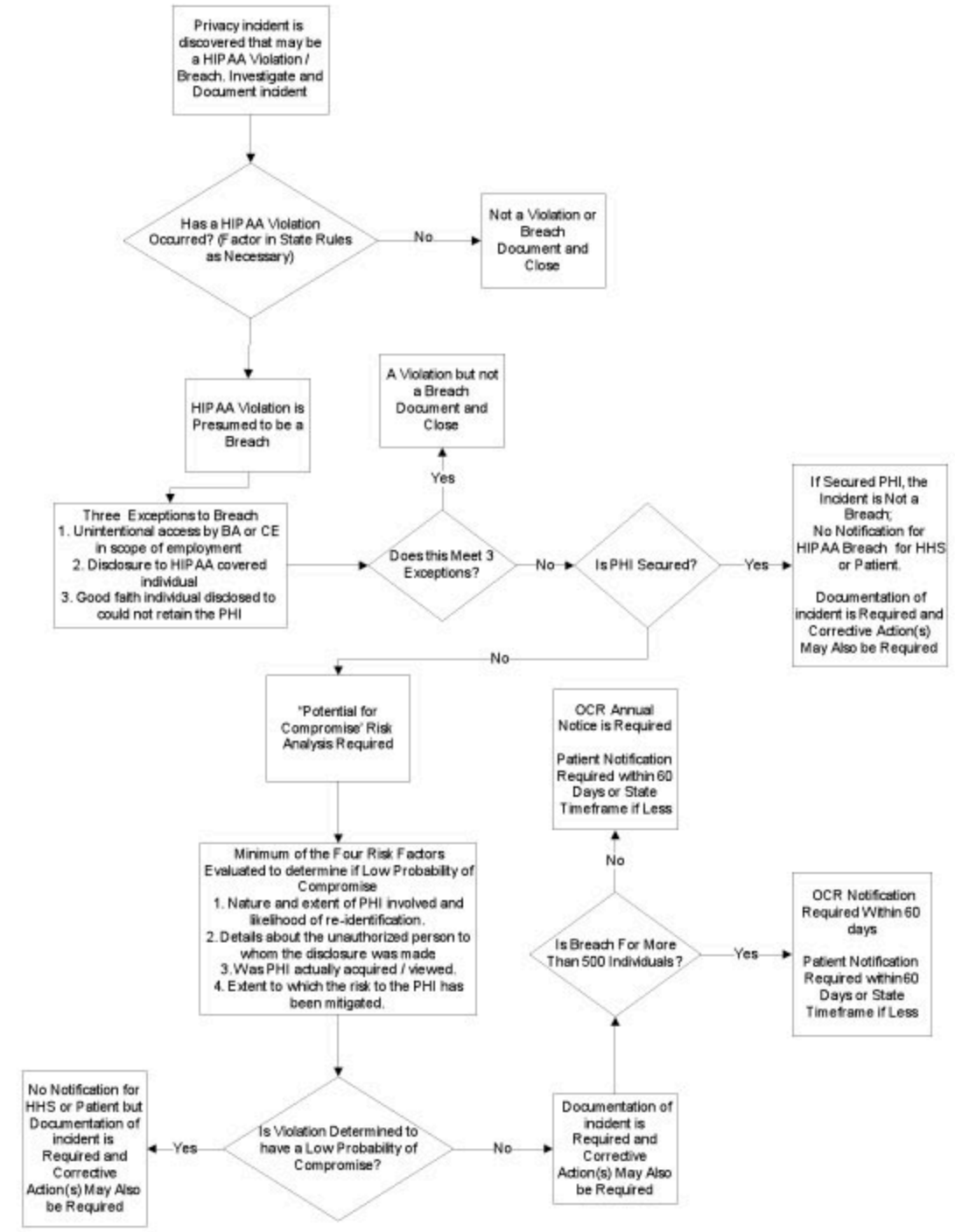
***NOTE**: Each incident will vary based on scenario and organizational policy and procedure. Therefore, each incident should be evaluated independently for probability of compromise. This tool may be used to help provide guidance in assessing risk factors and can be adapted to fit individual need.*

References

Department of Health and Human Services. "Guidance on Risk Analysis Requirements under the HIPAA Security Rule." July 14, 2010.

National Institute of Standards and Technology. "Information Security." Guide for Conducting Risk Assessments. September 2012.

Appendix C: Breach Decision Tree HIPAA PRivacy Breach Omnibus Final Rule



Prepared By

Rita Bowen, MA, RHIA, CHPS, SSGB
Rebecca Buegel, RHIA, CHP, CHC
Ben Burton, JD, MBA, RHIA, CHP
Kathy Downing, MA, RHIA, CHP, PMP
Jean T. Foster, RHIA
Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA
Kelly McLendon, RHIA, CHPS
Mary Poulson, RHIT, MA, CHC, CHPC
Nancy Prade, MBA, RHIA, CHPS
Angela Rose, MHA, RHIA, CHPS [note, this author was inadvertently left off the original list of authors in the print version]

Margaret (Peg) Schmidt, RHIA, CHPS
Diana Warner, MS, RHIA, CHPS, FAHIMA
LaVonne Wieland, RHIA, CHP

Acknowledgements

Barbara Beckett, RHIT, CHPS
Sheila D. Burgess, RHIA, CDIP, RN, HIT PRO-CP
Angie Comfort, RHIT, CDIP, CCS
Dana DeMasters, MN, RN
Julie Dooling, RHIA
Angie Fergen, RHIA, CHPS
Elisa R. Gorton, RHIA, CHPS, MAHSM
Lesley Kadlec, MA, RHIA
Michele Kruse, MBA, RHIA, CHPS
Wendy Mangin, MS, RHIA
Kim Turtle Dudgeon, RHIT, HIT Pro-IS/TS, CMT

The information contained in this practice brief reflects the consensus opinion of the professionals who developed it. It has not been validated through scientific research.

Article citation:
AHIMA. "Performing a Breach Risk Assessment - Retired" *Journal of AHIMA* 84, no.9 (September 2013): 66-70.
