HITECH Act
Breach Notification Risk Assessment Tool

Prepared by the
HCHICA Privacy, Security, and Legal Officials Workgroup

Summary of Breach Notification Rule

As required by the Privacy provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, under the American Recovery and Reinvestment Act of 2009 (ARRA), which was enacted on February 17, 2009, the OCR of the Department of Health and Human Services (HHS) has issued final regulations January 25, 2013, for breach notification by covered entities subject to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates (the “Omnibus rule”).

The final HITECH rule modifies the Privacy Rule, Security Rule, Breach Notification Rule, Genetic Information Nondiscrimination Act of 2008 (GINA), and the Enforcement Rule. These regulations require HIPAA covered entities to provide breach notification in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised (or one of the other exceptions to the definition of breach applies).

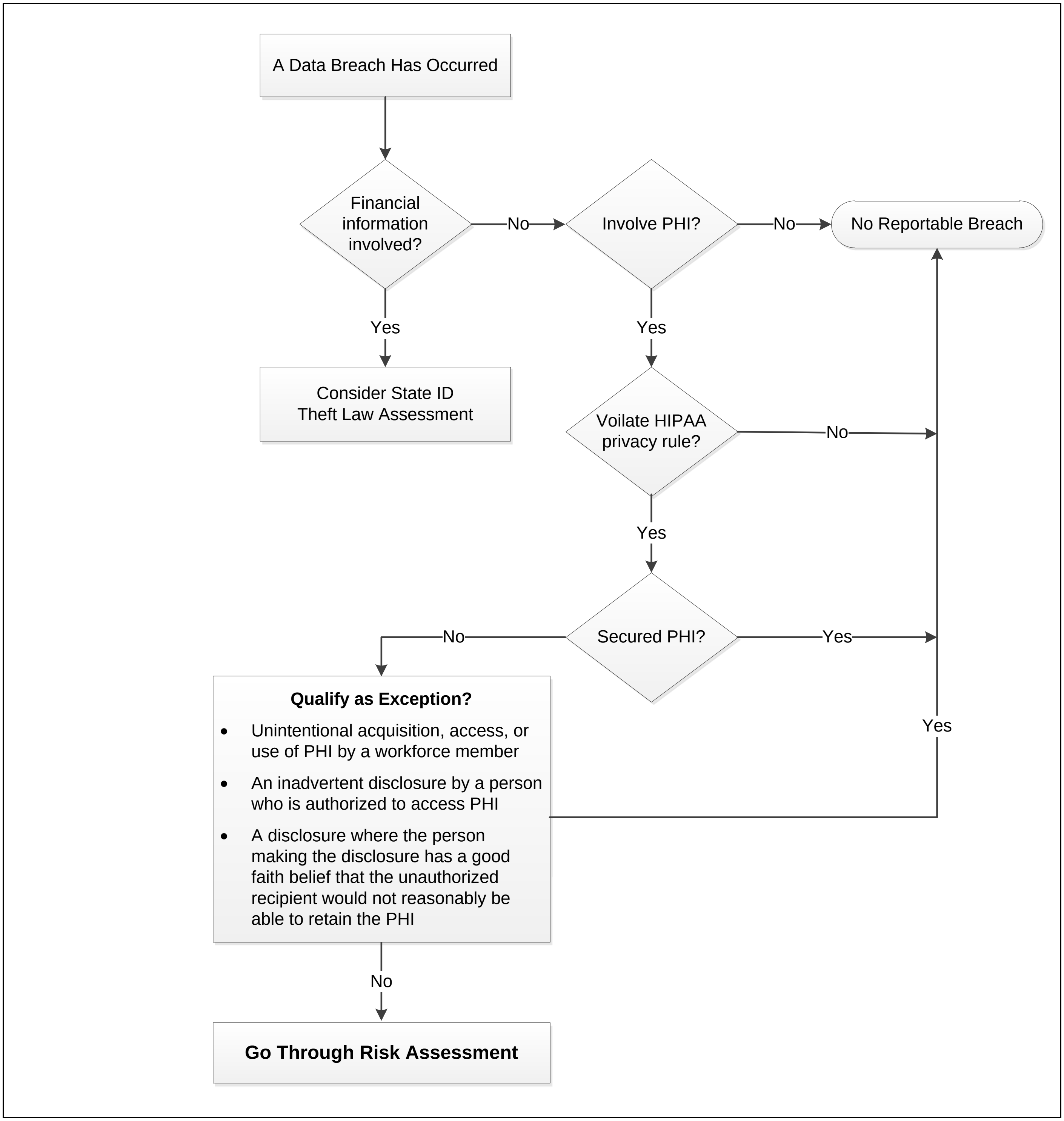
In addition, in some cases the covered entity is required to provide notification to the media of breaches. In the case of a breach of unsecured protected health information (PHI) at or by a business associate of a covered entity, the business associate is required to notify the covered entity of the breach. Finally, it is required that the Secretary post on an HHS website a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.

Risk Assessment Tool Introduction

The Breach Notification Final Omnibus Rule requires covered entities, business associates, and subcontractors to perform and document risk assessments on breaches of unsecured protected health information (PHI) to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised. In performing the risk assessment covered entities, business associates, and subcontractors may need to consider a number or combination of factors. The Risk Assessment Tool provides guidelines for performing these risk assessments.

The following chart can be used to assist in determining if an actual breach occurred. If the initial circumstances confirm a breach occurred and do not fit the noted exceptions, then you should proceed to the actual risk assessment to determine if the breach is notifiable.

Breach Flow


A Data Breach Has Occurred
Financial information involved?
No
Involve PHI?
No
No Reportable Breach
Yes
Yes
Consider State ID Theft Law Assessment
Voilate HIPAA privacy rule?
No
Yes
Secured PHI?
No
Yes
Qualify as Exception?
• Unintentional acquisition, access, or use of PHI by a workforce member
• An inadvertent disclosure by a person who is authorized to access PHI
• A disclosure where the person making the disclosure has a good faith belief that the unauthorized recipient would not reasonably be able to retain the PHI
Yes
No
Go Through Risk Assessment

Iowa DHS Breach Notification Risk Assessment Tool

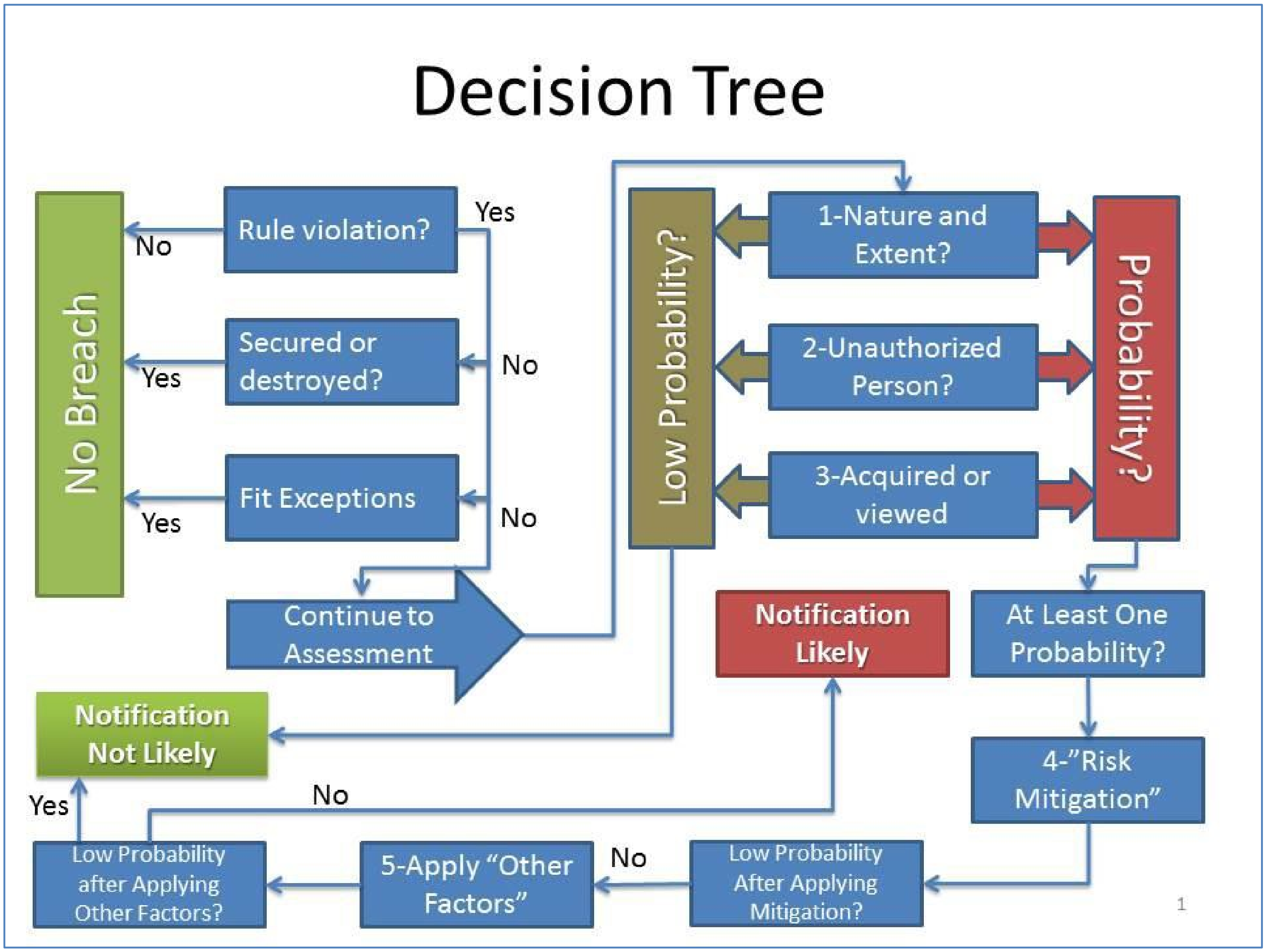
Incident/File/Name		
Event Date	Discovery Date	Number of Individuals Affected
Point of Contact		Phone Number
Brief Summary/Findings		
Final Decision		

Source of incident: Who was responsible for the inappropriate acquisition, access, use or disclosure (incident)?	Internal to Your Organization or Business Associate
If a business associate or subcontractor is the source of the incident, enter the date the business associate or their business associate made you aware of the incident.	Date
Is there a BAA or other agreement in place? Have they performed a breach assessment of their own? Have any notifications been made by the BA or subcontractor?	□ Yes □ No □ Yes □ No □ Yes □ No
Are you the business associate or subcontractor?	□ Business associate □ Subcontractor
When was it discovered or when should it have been discovered?	Date
If you are the Business Associate or subcontractor, enter the date you notified the other Covered Entity of the incident.	Date
Enter the date that our organization became aware of the incident.	Date

Section 164.410(a)(2) further provides that a covered entity is 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 covered entity (determined in accordance with the federal common law of agency).

This Decision Tree illustrates a conceptual method of working through the risk assessment including any exceptions. Since the new breach notification standard assumes a compromise, the goal in every risk factor should be to obtain a "low probability." For that reason, the scoring or outcome only has two options. Through your deliberations you will either reach a low probability or not.

If any of the first three risk factors are rated as "Probable," proceed to use "Mitigation Factors" to see if the result remains the same. If all factors are reduced to "Low Probability," notification is not likely. If all are not reduced, you should use the elements in the "Other Factors" to try to further reduce the likelihood to "Low Probability." It is further understood that one factor can be so serious of egregious as to act as a circuit breaker that will force breach notification. Our recommendation is to work through the entire assessment even though a decision may be made early in the process.



It should be duly noted that the elements and considerations assigned to each risk factor are not intended to be an exhaustive list. There may be other factors that should be considered as the tool is not designed to limit additional factors not currently anticipated. Some agencies will use this tool as their only documentation of an event and should ensure any additional elements utilized are memorialized for future justification or review. Another tendency is to prematurely score higher because your circumstances fit an example given in the rule. Use the entire tool to your benefit. As guidance in the final rule states, *"The risk assessment should involve consideration of all of these factors, in addition to, others that may be relevant. One factor is not necessarily determinative, and some factors may offset or outweigh others, depending on the circumstances."* (See 78 F.R. 5643).

Section 1. NCHICA Breach Notification Risk Assessment Tool

1. Is there a HIPAA privacy or security rule violation involving the acquisition, access, use or disclosure of PHI?

   ☐ Yes ☐ No

   *If **No**, then **STOP** here. No breach has occurred.*

   *If **Yes**, then proceed to the next question.*

2. Was data secured or properly destroyed in compliance with the requirements which state only encryption and destruction, consistent with National Institute of Standards and Technology (NIST) guidelines 13402(h)(2) under public law 111-5, renders protected health information unusable, unreadable or indecipherable to “unauthorized persons.”

   ☐ Yes ☐ No

   *If **No**, then **STOP** here. No breach has occurred.*

   *If **Yes**, then proceed to the next question.*

3. Does this incident qualify under one of the following exceptions?

   ☐ Yes ☐ No

   - **An unintentional acquisition, access or use of PHI by a workforce member** if such acquisition, access or use was made in good faith and within the scope of the workforce member's authority and does not result in further use or disclosure not permitted by the privacy rules. (45 C.F.R. § 164.402). For example, no notification is required where an employee mistakenly looks at the wrong patient’s PHI but does not further use or disclose the PHI.
   - **An inadvertent disclosure by a person who is authorized to access PHI** to another person authorized to access PHI at the same covered entity or business associate, and the PHI is not further used or disclosed in a manner not permitted by the privacy rules. (*Id.*). For example, no notification is required if a medical staff member mistakenly discloses PHI to the wrong nurse at a facility but the nurse does not further use or disclose the PHI improperly.
   - **A disclosure where the person making the disclosure has a good faith belief that the unauthorized recipient would not reasonably be able to retain the PHI.** (*Id.*). For example, no notification is required if a nurse mistakenly hands PHI to the wrong patient but immediately retrieves the information before the recipient has a chance to read it.

   *If **No**, then **STOP** here. No breach has occurred.*

   *If **Yes**, then proceed to the next question.*

**If you did not hit a STOP above in Section 1,
then work through the rest of the assessment to determine whether
there is a low probability that the PHI has been compromised.**

Go to Section 2.

Section 2. NCHICA Breach Notification Risk Assessment Tool

Risk Assessment Factors	Circumstances of the Incident			
	Considerations	Elements		Score
1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. For example, if a file of known abuse victims is breached that includes the victims' addresses, then you will probably want to rank the breach of this data as a high probability of causing harm to the person(s) impacted by the breach. However, under other circumstances, just the release of an address may be considered a low risk of harm to the person(s) impacted by the breach.[1]		Clinical Information • Name • MRN • Address • Room number • Email • DOB • Provider • Date of service • Limited data set • Non-diagnostic information • Other	Consider the risk of re-identification.	Low Probability
		• SSN • Sensitive diagnosis information • Sensitive protected health information which may include information about sensitive diagnosis such as HIV, substance abuse, and/or mental health • STD • Medications that indicate sensitive diagnosis • Other		Probability

[1] *All examples cited are from the narrative in the final rule.*

Risk Assessment Factors	Circumstances of the Incident		
	Considerations	Elements	Score
2. The unauthorized person who used the PHI or to whom disclosure was made. If the information impermissibly used or disclosed is not immediately identifiable, entities should determine whether the unauthorized person who received the protected health information has the ability to re-identify the information. For example, if information containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low probability that the protected health information has been compromised. (78 F.R. 5643). Does recipient have confidentiality obligations? (5643)		• Your business associate • Another covered entity • Internal workforce • Wrong payor (not the patient's) • Unauthorized family member • Other	Low Probability
		• Non-covered entity • Media • Unknown, lost, or stolen • Member of the general public • Patient's employer • Other	Probability
3. Whether the PHI was actually acquired or viewed. For example, there is likely a low risk if a misdirected letter is returned unopened or a lost computer is recovered and it is confirmed that PHI was not accessed. Conversely, there is a higher risk where the recipient opens and reads a misdirected letter even though she reports the letter to the covered entity.		• Unauthorized internal acquisition, access, and/or use without disclosure outside of organization. • Extent to which PHI was in fact **accessed** (5643) • Verbal disclosure • View only • Other	Low Probability
		• Paper/fax • Electronic • Other	Probability

Risk Assessment Factors	**Circumstances of the Incident**	
	Disposition	**Elements**
4. Whether the risk to the PHI has been mitigated. For example, there may be a lower risk if a fax is directed to the wrong number, but the recipient confirms: • That they returned or destroyed the PHI; • The PHI has not been and will not be further used or disclosed; and • The recipient is reliable. (*Id.*). This factor highlights the need for covered entities and business associates to immediately identify and respond to potential breaches to reduce the probability that PHI is compromised and the necessity of breach reporting.	**Disposition** (What happened to the information after the initial disclosure?) Has the risk to the PHI been mitigated? *Did we get it back?* *Certification/attestation of destruction?* *Reliability of attestation?* *Unreadable/undecipherable?* *Other impact?* *Controls in place to influence ability to compromise?* *Flag records like red flags?* *Value of data? (insurance number vs. other types)*	• Visual; viewed only with no further disclosure or retention • Obtained reliable assurances that the use or disclosure was very limited • Obtained reliable assurances that the PHI will not be further used or disclosed • Information returned complete • Information properly destroyed and attested to • Information properly destroyed (unattested) • Electronically deleted (unsure of backup status) • Other

Risk Assessment Factors	**Additional Controls**
5. Other factors.	• Electronic data wiped • Information/device encrypted, but does not meet compliance with NIST standards • Hard copy or electronic media destroyed, but does not meet compliance with NIST standards • Encrypted; encryption keys not secured • Password protected • No controls
	Safeguards listed in the DHHS Breach Reporting form.
	• Firewalls, packet filtering (router-based) • Secure browser sessions • Strong authentication • Encrypted wireless, physical security • Logical access control • Anti-virus software, intrusion detection • Biometrics • Other

Additional information considered in your determination:

Analysis Points/Narrative

Ensure mitigation or process correction within 30 days for reoccurrence:

Scoring

If the entity concludes that the risk assessment demonstrates a low probability that the PHI has been compromised, the entity should document its analysis and may forego breach notification. On the other hand, if the risk assessment fails to demonstrate a low probability that the PHI has been compromised, the entity is required to report the breach unless one of the regulatory exceptions applies.

The scoring is meant to serve only as a guide in decision making and not designed to make the notification decision for you. There are a variety of factors and mitigations that may be involved in your incident that this tool may not foresee or predict. An attempt was made to develop this in a way that would help you in documenting your actions, consider risk factors and circumstances, and then aid in your final decision of whether or not to make a breach notification. There is no “scoring” element for factors 4 and 5 as they were considered mitigation factors as opposed to risk factors.

The scoring is designed to be subjective enough so that each entity can consider their own policies, technical safeguards/constraints, mitigation strategies, interpretation, and details specific to the specific incident they are reviewing.

The risk factors carry a possible outcome of “Low Probability” or “Probability.”

Probability of Compromised Information

Low Probability ◄		► **High Probability**
Notification Unlikely	Articulate and Document Decision To Notify or Not	Notification Likely

Breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised

Addendum “B” HITECH Definitions (164.402)

Breach

The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information:

(1) (i) For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

(2) Breach excludes:

(i) Any unintentional acquisition, access or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, 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 under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care 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 under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate 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.

Unsecured Protected Health Information

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 111-5.