



Federal Breach Notification Decision Tree and Tools

Disclaimer

This document is copyright 2009 by the Long Term Care Consortium (LTCC). These materials may be reproduced and used only by long-term health care providers and their health care affiliates for their internal use, in connection with their efforts to comply with relevant legal rules and regulations. All other reproduction, transfer and use is prohibited without the express written consent of the LTCC. Neither the LTCC nor its members make any representation that use of these materials will ensure other legal compliance.

LTCC Mission Statement

To provide leadership and guidance to the long term care profession utilizing the member organizations' collective knowledge, expertise and information resources to improve overall compliance efforts and reduce the overall burden of compliance through collaboration on important initiatives that are common to the profession.

Breach Notification Overview

On August 24, 2009, the Department of Health & Human Services' Breach Notification for Unsecured Protected Health Information Interim Final Rule (Federal Breach Notification Rule) was published in the Federal Register as required by the American Recovery & Reinvestment Act of 2009. The new federal breach reporting requirements apply to HIPAA covered entities and their business associates. It requires covered entities to notify individuals whose unsecured protected health information (PHI) has been accessed, acquired or disclosed because of a breach, which is defined as "the unauthorized acquisition, access, use or disclosure of PHI." The rule also outlines a few exceptions to the definition of a breach.

To determine whether a breach has occurred, covered entities and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the resident as a result of an impermissible use or disclosure. After a breach has been discovered, affected residents must be notified of the breach without unreasonable delay and no later than 60 days. Breaches affecting more than 500 residents must be reported immediately to HHS and the media. Breaches affecting less than 500 residents are logged and reported to HHS on an annual basis. When

calculating the number of affected residents, take into consideration the structure of the organization – all reporting is at the covered entity level.

The rule provides updated guidance specifying the technologies and methodologies that render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals and therefore not subject to the notification requirements because the information does not meet the “unsecured protected health information” criteria.

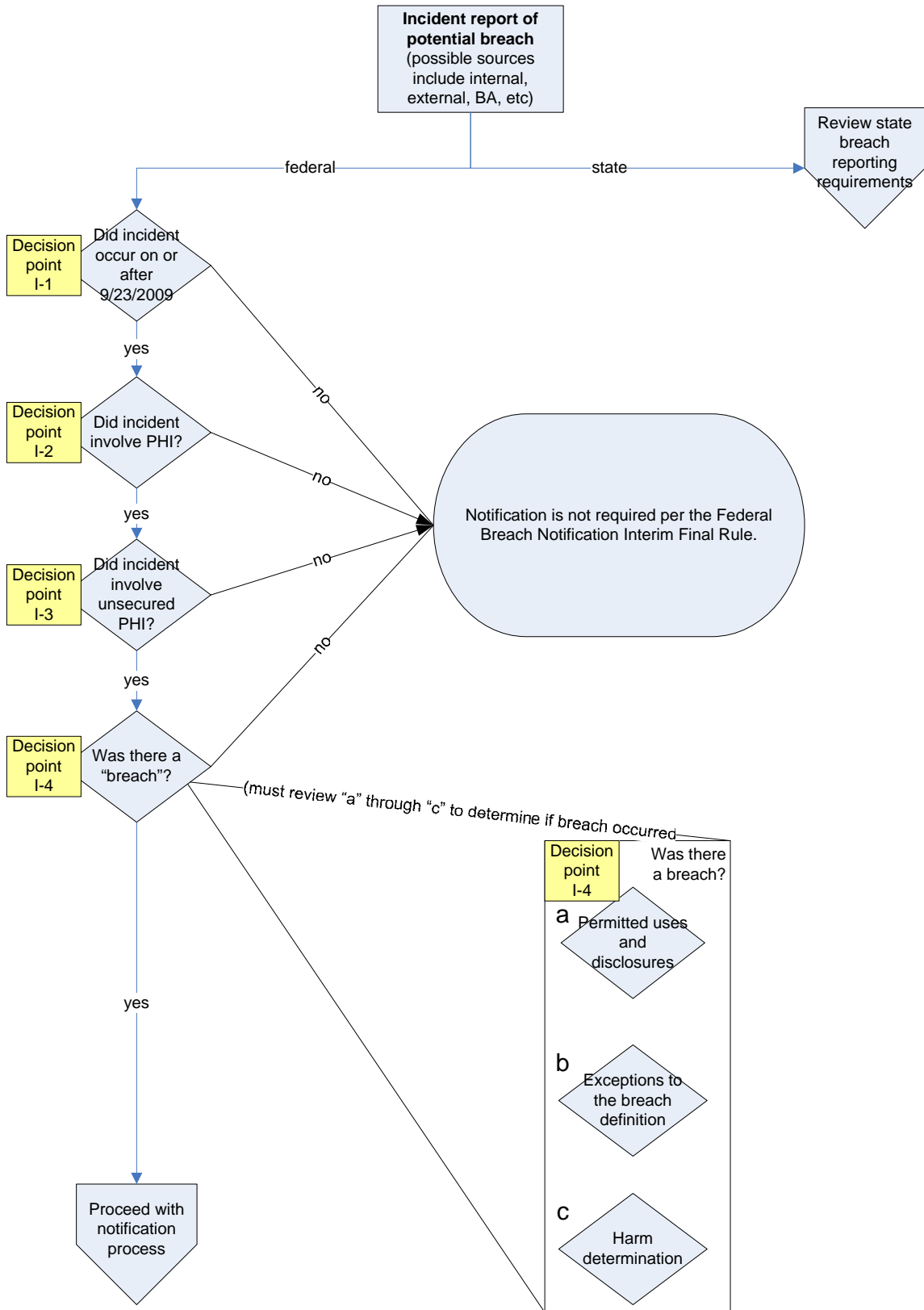
Using the Decision Tree and Tools

This document serves as a guide to determine if a reported incident involves a breach of PHI information in a manner that requires notification of the affected residents and what method of notification is required under the federal breach regulation. This document does not address state security breach notification requirements.

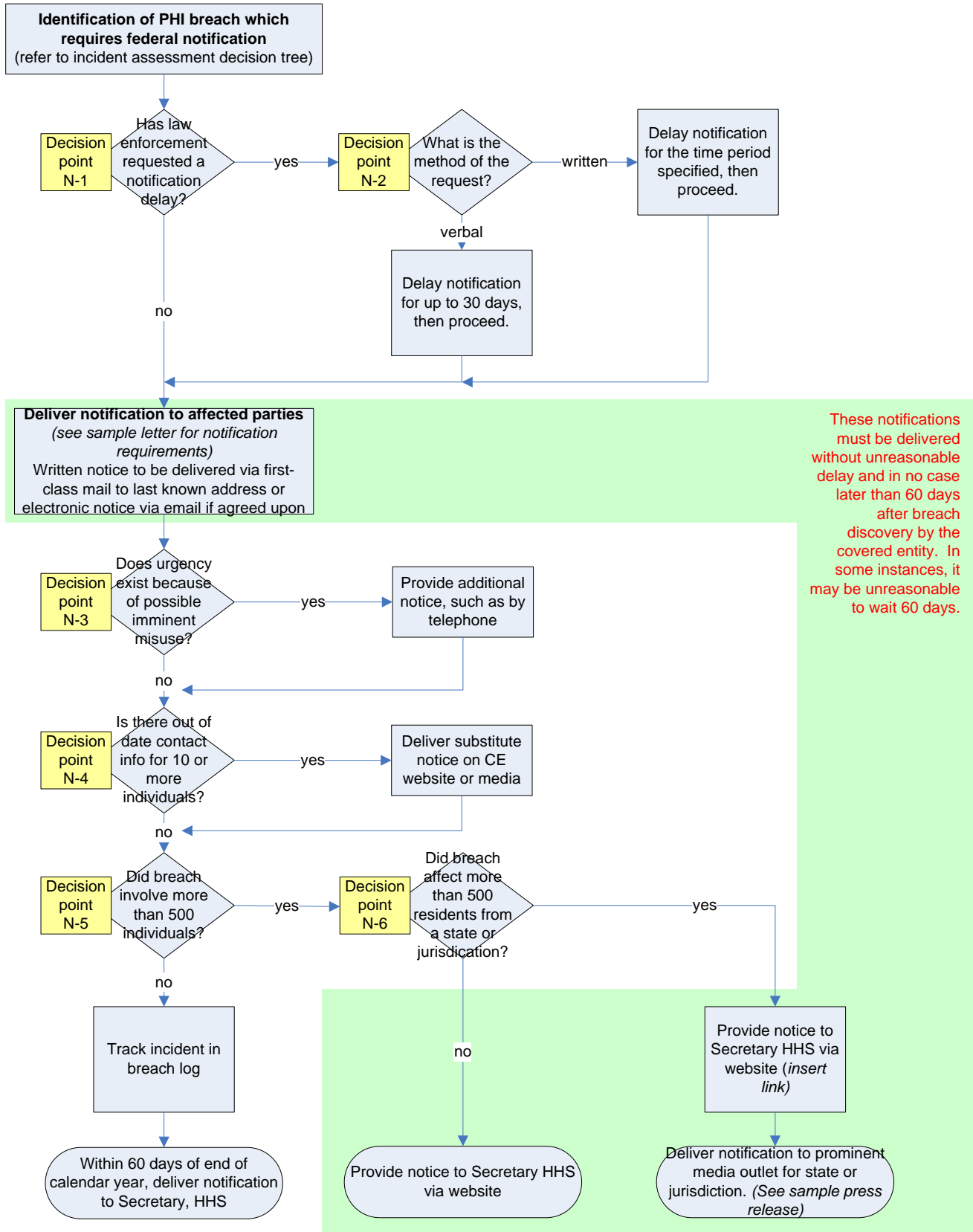
Each decision point references additional information on subsequent pages which may be useful throughout the assessment of an incident. You will need to document your assessment process to support your conclusions. Though you may conclude that notification is not required under federal law, you should review any applicable state laws as well as your organization’s policies and procedures to assess whether it is prudent to proceed with notification even though it may not be required.

Sample notification letters to affected residents and the media are available on the LTCC site for your reference.

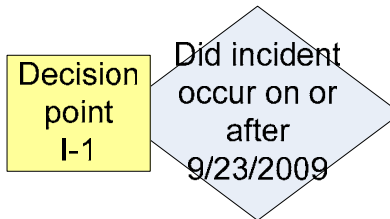
Incident Assessment



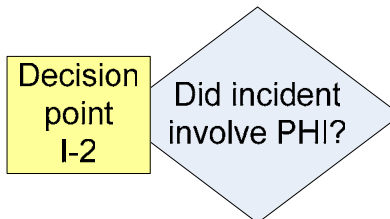
Notification Process



Incident Assessment Decision Points



The effective date of this interim final rule is September 23, 2009. Notification requirements apply to breaches that occurred on or after September 23, 2009.



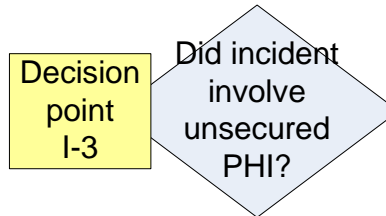
The HIPAA Rules define “protected health information” as the individually identifiable health information held or transmitted in any form or medium by HIPAA covered entities and business associates.

Excluded from the definition of PHI is de-identified information as defined in the HIPAA Privacy Rule and listed below:

De-identified health information: Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information (see section 164.514(a) or glossary).

Limited Data Sets: A limited data set is protected health information that excludes the direct identifiers of the individual or of relatives, employers, or household members of the individual. See the glossary for a list of the identifiers.

The Federal Breach Notification Rule contains a narrow, explicit exception to a breach if the limited data set also excludes date of birth and zip code, because it does not compromise the security or privacy of PHI.



Due to the variations in each entity’s environment, no uniform standards exist for secured Protected Health Information. Each covered entity must perform a risk assessment to determine if PHI is secured.

The Federal Breach Notification Rule applies to unsecured PHI. The generally accepted definition of secured PHI is PHI that is rendered unusable, unreadable, or indecipherable to unauthorized individuals. Notification is not required for PHI that is considered secure. Section II in the Federal Breach Notification Rule contains guidance specifying the technologies and methodologies that render PHI secure.

PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of a(n)...process to transform data into a form in which there is a low probability of assigning meaning (to the data) without use of a confidential process or key” (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached.

To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data that they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

These publications were cited as potentially valuable resources, although not required by CMS, for technical personnel having knowledge of the covered entity’s IT environment with specific questions and concerns about securing PHI.

- (i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, [Guide to Storage Encryption Technologies for End User Devices](#).¹

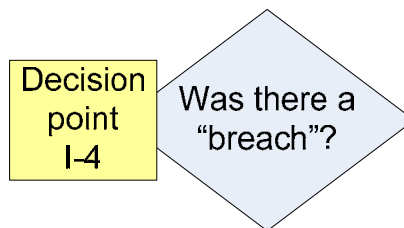
¹ (<http://www.csrc.nist.gov/>)

(ii) Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, [Guidelines for the Selection and Use of Transport Layer Security \(TLS\) Implementations](#)¹; 800-77, [Guide to IPsec VPNs](#); or 800-113, [Guide to SSL VPNs](#)¹, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

(i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of destruction.

(ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, [Guidelines for Media Sanitization](#)¹ such that the PHI cannot be retrieved.



In order for a use or disclosure of resident information to be considered a breach, the acquisition, use or disclosure of the PHI must be in violation of the HIPAA Privacy Rule. Permissible uses and disclosure under the Privacy Rule must fall into one of the categories below.

The following are questions you must ask and answer as you document your efforts in confirming a breach or validating a permissible use or disclosure.

PERMITTED USES AND DISCLOSURES

1. Was the PHI accessed, acquired, used or disclosed for treatment, payment or healthcare operations purposes (refer to your notice of privacy practices)?

If No, go to question #2

If Yes, and the purpose was for treatment, it is not a breach.

If Yes, and the purpose was for payment or healthcare operations, was the PHI the minimum necessary amount for the given task?

If Yes, it is not a breach.

If No, go to the section **Harm Determination**.

2. Was the PHI acquired, used or disclosed incidental to a permitted use or disclosure?

In order for a use or disclosure to be considered incidental, it must be related to a use or disclosure that is either permitted or required under the Privacy Rule and the amount of information must have been the minimum necessary for the intended purpose and reasonable safeguards must have been taken to keep the information confidential. For example, the following practices are permissible under the Privacy Rule, if reasonable precautions were taken to minimize the chance of incidental disclosures to others who may be nearby:

- a. Health care staff may orally coordinate services at nursing stations.
- b. Nurses or other health care professionals may discuss a resident's condition over the phone with a provider or legal representative.
- c. A health care professional may discuss lab test results with a resident or other provider in a joint treatment area.
- d. A physician may discuss a residents' condition or treatment regimen in the resident's semi-private room.

If Yes, it is not a breach.

If No, go to question 3.

3. Was the PHI disclosed pursuant to and in compliance with a HIPAA-compliant authorization?

If Yes, it is not a breach.

If No, go to question 4.

4. Was the PHI accessed, acquired, used or disclosed for facility directory purposes in compliance with 164.510(a)?

If Yes, it is not a breach.

If No, go to question 5.

5. Was the PHI accessed, acquired, used or disclosed for involvement in the resident's care and notification purposes in compliance with 164.510(b)?

If Yes, it is not a breach.

If No, go to question 6.

6. Was the PHI accessed, acquired, used or disclosed pursuant to 164.512 uses and disclosures for which an authorization or opportunity to agree or object is not required? Was it:

- a. required by law,
- b. for public health activities,
- c. about victims of abuse, neglect or domestic violence,
- d. for health oversight activities,
- e. for judicial and administrative proceedings,
- f. for law enforcement purposes,
- g. about decedents,
- h. for cadaveric organ, eye or tissue donation purposes,
- i. for research purposes,
- j. to avert a serious threat to health or safety,
- k. for specialized government functions, OR
- l. for workers' compensation purposes, AND
- m. in compliance with the requirements outlined in 164.512?

If Yes, it is not a breach.

If No, go to question 7.

EXCEPTIONS TO THE BREACH DEFINITION

Does the impermissible access, acquisition, use or disclosure fall under one of the following exceptions?

7. Was it an incidental access, use or disclosure by a workforce member of the covered entity or business associate:
- a. While acting under the organization's authority, and
 - b. Made in good faith, and
 - c. Within their scope of authority, and
 - d. Does not result in a further use or disclosure?
 - i. For example, a billing employee receives and opens an e-mail containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it. The billing employee unintentionally accessed protected health information to which he was not authorized to have access. However, the billing employee's

use of the information was done in good faith and within the scope of authority, and therefore, would not constitute a breach and notification would not be required, provided the employee did not further use or disclose the information accessed in a manner not permitted by the Privacy Rule.

If Yes, there is no breach.

If No, go to question 8.

8. Was it an inadvertent disclosure:
- a. By a person who is authorized to access protected health information at a covered entity or business associate,
 - b. 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
 - c. The information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the Privacy Rule?
 - i. For example, a nurse calls a doctor who provides medical information on a resident in response to the inquiry. It turns out the information was for the wrong resident and the information was not further used or disclosed by the doctor.

If Yes, there is no breach.

If No, go to question 9.

9. Was it 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?
- i. For example, a medical records' clerk hands a resident a copy of a medical record, but quickly realizes that it was another resident's record and requests the return of the record. In this case, if the medical records clerk can reasonably conclude that the resident could not have read or otherwise retained the information, then providing the medical record to the wrong resident does not constitute a breach.

If Yes, there is no breach.

If No, proceed to question 10.

HARM DETERMINATION

10. Was the PHI accessed, acquired, used or disclosed by another entity governed by the HIPAA Privacy and Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 and Federal Information Security Management Act (FISMA) of 2002?

If Yes, were immediate steps taken to mitigate the impermissible use/disclosure/acquisition? For example:

- a. Was the recipient contacted and were satisfactory assurances obtained assuring that the PHI would not be further used or disclosed or would be destroyed? Or
- b. Was the PHI not accessed, opened, altered, transferred or otherwise compromised? For example, a mailing is returned unopened or through analysis it is determined that information on a laptop or computer was not accessed.

If Yes, and the steps above eliminated or reduced the risk of harm to the individual to a less than significant risk, then we interpret that the security and privacy of the information has not been compromised and, therefore, no breach has occurred.

If No, go to question 11.

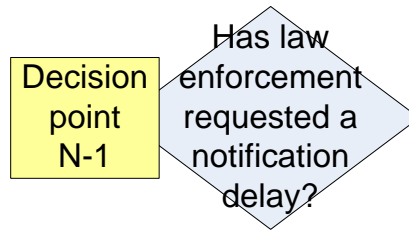
11. Does the type or amount of PHI accessed, acquired, used or disclosed pose a significant risk of financial, reputational or other harm to the resident?
- a. Was only minimal PHI acquired, accessed, used or disclosed such as just the patient name and the fact that services were received?
 - b. Did the PHI include the resident's name and type of services received? For example: were services from a specialized facility such as an infectious disease clinic or substance abuse provider?
 - c. Did the PHI include high risk information that could be used for identity theft such as name, social security number, date of birth, financial or credit card account numbers, driver's license number or state-issued identification card number or maiden name?
 - d. Did the PHI include only a limited data set as defined by the Privacy Rule and the likelihood of re-identification is low? For example, if the information included the zip code for a metropolitan city vs. a rural location.

If the type or amount of PHI that was accessed, acquired, used or disclosed DOES NOT pose a significant risk of financial, reputational or other harm to the resident, then we interpret that the security and privacy of the information has not been compromised and, therefore, no breach has occurred.

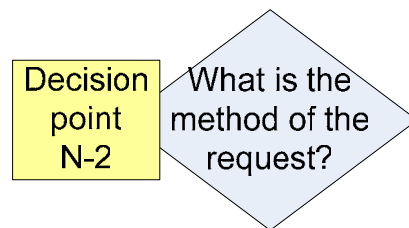
If the type or amount of PHI that was accessed, acquired, used or disclosed DOES pose a significant risk of financial, reputational or other harm to the resident, then there IS likely a breach.

Continue the investigation and document your decision.

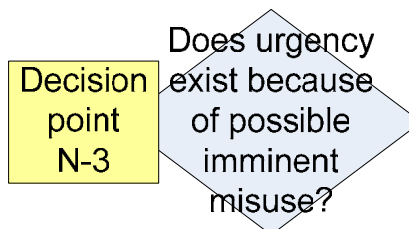
Notification Process Decision Points



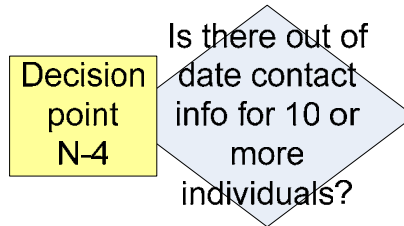
If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting would impede a criminal investigation, or cause damage to national security, notification should be delayed.



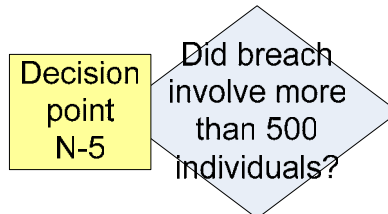
Law enforcement requests are accepted in two formats: written statement or oral statement. If the type of request is oral, the covered entity should delay notification for a period of up to 30 days, then proceed with the notification process. If the request is written, the request should specify a time frame for the delay. The covered entity should honor the request and delay notice as specified.



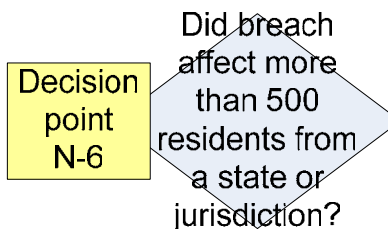
In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured PHI, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to the standard notice.



In the case where there is insufficient or out-of-date contact information for ten or more affected individuals, a substitute notice is required. This substitute notice must be provided in the form of a media announcement or conspicuous posting for a period of 90 days on the covered entity's web site home page.



Based upon the number of individuals affected by the breach, additional notice may be required. Determine the number of affected individuals and proceed accordingly.



Where a breach affects more than 500 residents from a state or jurisdiction, additional notice is required. In that case, the covered entity shall notify prominent media outlets serving the state or jurisdiction.

.....

REFERENCES

American Recovery and Reinvestment Act of 2009 (ARRA):

- Final text of legislation (HITECH = Title VIII)
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf

Federal Breach Notification Rule:

- General information
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>
- Interim final rule
<http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>
- Breach notification guidance
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>
- Guidance for securing PHI
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>
 - Encryption of data at rest – NIST 800-111
 - Encryption of data in motion (TLS) – NIST 800-52
 - Encryption of data in motion (VPN) – NIST 800-113
 - Guidelines for media sanitation – NIST 800-88
<http://www.csrc.nist.gov/publications/PubsSPs.html>
 - Cryptographic security – FIPS 140-2
<http://www.csrc.nist.gov/publications/PubsFIPS.html>

Instructions for submitting notice to the secretary:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>