

HHS and FTC Dive Deeper Into the Breach: Update on Breach Notification Under the HITECH Act

SHARON R. KLEIN | KLEINS@PEPPERLAW.COM

REBEKAH A. Z. MONSON | MONSONR@PEPPERLAW.COM

M. PETER ADLER*

REPRINTED WITH PERMISSION FROM THE NOVEMBER 2009 ISSUE OF THE *PRIVACY & DATA SECURITY LAW JOURNAL*. COPYRIGHT © 2009 ALEXESOLUTIONS, INC. FOR FURTHER INFORMATION, SEE [HTTP://WWW.ASPRATT.COM/STORE/L87.PHP](http://www.aspratt.com/store/L87.php) OR CALL 1.800.572.2797.

The Federal Trade Commission (FTC) and the U.S. Department of Health and Human Services (DHHS) each recently issued final breach notification regulations governing entities covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) along with vendors of personal health records (PHR) and related entities that are not subject to the HIPAA requirements. These final regulations are required under the Health Information Technology for Economic and Clinical Health (HITECH) Act signed into law on February 17, 2009, as Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA).

As has been widely discussed in recent months, ARRA made many changes to the privacy and security of health information including establishing a federal standard for breach notifications in the health care industry. While HIPAA addressed privacy and security of protected health information (PHI), HIPAA did not include requirements for HIPAA-covered entities to notify individuals in the event of breaches of their PHI. With the publication of these latest regulations the FTC and DHHS have finalized the breach notification requirements mandated by the HITECH Act and have responded to many comments received on the proposed rules issued back in April 2009.

AS NOTED IN OUR PRIOR ARTICLE ON THIS TOPIC, HEALTH CARE ENTITIES, ESPECIALLY BUSINESS ASSOCIATES, SHOULD CAREFULLY ANALYZE THEIR NEED FOR DATA TO BE PERSONALLY IDENTIFIED AND LOOK FOR WAYS TO PROPERLY DE-IDENTIFY PHI SO THAT SUCH DATA STREAMS ARE OUTSIDE REGULATORY PURVIEW. THE DHHS IS TO ISSUE FURTHER GUIDANCE ON DE-IDENTIFICATION BY FEBRUARY 17, 2010.

DHHS INTERIM FINAL RULE

Section 13402 of the HITECH Act includes the breach notification obligations for HIPAA-covered entities and their business associates for breaches of “unsecured” PHI (including methods of notification, timeliness, content of the notice, etc.). The DHHS issued an interim final rule implementing these requirements on August 19, 2009.¹ As required by the HITECH Act, these regulations were issued as interim final regulations, how-

* MR. ADLER IS CHIEF PRIVACY OFFICER AT UNITEDHEALTH GROUP. HE IS A FORMER PARTNER AT PEPPER HAMILTON LLP.

This publication may contain attorney advertising.

ever, the DHHS is providing the public with a 60-day comment period. While these rules apply to breaches that occur on or after September 23, 2009, DHHS has provided for a six-month delay in enforcement and has noted that it will use its enforcement discretion to not impose sanctions for failure to provide required notifications for breaches that are discovered before February 22, 2010.

What Is, and Is Not, a Breach

In order to determine whether a HIPAA-covered entity or business associate is required to make a notification, it is necessary to determine whether there has been a “breach” of “unsecured PHI.” The interim final rule defines a “breach” as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule and that compromises the security or privacy of the PHI. In the event of an asserted breach of information, covered entities will need to affirmatively answer several questions before addressing the notification requirements under the new rules: (1) was PHI involved, (2) was the PHI “unsecured,” and (3) was there a “breach” that passed the harm threshold as described later in this article?

The DHHS interim final rule’s definition of “breach” only applies to PHI. Individually identifiable health information excluded from the HIPAA definition of PHI, such as employment records held by a HIPAA-covered entity in its role as an employer and certain student records, are not PHI and therefore are not subject to the new requirements. While the DHHS breach notification rule may not apply to such identifiable information, the covered entity will need to consider whether other notification laws do apply. Additionally, individually identifiable health information that has been de-identified in accordance with the HIPAA Privacy Rule requirements are not PHI and therefore not subject to the DHHS breach notification requirements.

By definition a breach requires the acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule. A violation of the HIPAA Security Rule will not itself constitute a potential breach; however, that same violation may lead to a use or disclosure of PHI not protected under the Privacy Rule, which in turn may be a potential breach. Moreover, not all violations of the HIPAA Privacy Rule will be breaches under these new requirements. Even if PHI has been acquired, accessed, used or disclosed in violation of the HIPAA Privacy Rule, in order for that violation to result in a breach the violation must pose harm to the individual. The second part of the

“breach” definition includes this harm threshold; to be a breach the violation must be one “which compromises the security or privacy of the PHI,” which means it “poses a significant risk of financial, reputational, or other harm to the individual.” Covered entities will need to perform a risk assessment to determine if there has been significant risk of harm to individuals as a result of the impermissible use or disclosure of PHI. The DHHS provides some guidance in the preamble to the interim final rule on possible factors to consider:

- who impermissibly used, or to whom the information was impermissibly disclosed — if the recipient of the information is obligated to protect the privacy and security of the information
- if the effect of the impermissible disclosure can be mitigated so that the risk of harm to the individual is less than a “significant” risk
- if the impermissibly disclosed information was returned prior to being accessed for an improper purpose — an example provided in the preamble is if a lost or stolen laptop is returned and forensics investigation reveals no improper use
- covered entities and business associates should consider the type and amount of PHI involved in the impermissible use or disclosure. Particular attention should be paid to information that may be considered sensitive for reputational harm and employment discrimination (such as substance treatment, oncology services, mental health, etc.).
- the DHHS comments also refer readers to the OMB Memorandum M-07-16 for examples of other factors to consider.

Covered entities and business associates have the burden of demonstrating that no breach has occurred. It is critical that the risk assessment be documented so that, if necessary, a covered entity or business association can demonstrate that no breach notification was required following an impermissible use or disclosure of PHI.

With respect to limited data sets, defined in the HIPAA Privacy Rule as PHI that excludes 16 direct identifiers but is not fully de-identified, the DHHS concluded that due to the risk of re-identifying such information, impermissible uses or disclosures of limited data sets can be a breach and thus need to be evaluated to determine the risk of harm to an individual. Such

a risk assessment should take into consideration the risk of re-identification of the PHI contained in the limited data set. The interim final rule also includes a narrow explicit exception for PHI that is a limited data set and also excludes birth date and zip code information — impermissible use or disclosure of such information will be deemed to not compromise the security or privacy of PHI. The DHHS concluded that if such information has a low level of risk, however, they are soliciting comments on this narrow exception. Uses of limited data set information that include birth date and zip code information continue to be permitted; however, in the event there is an alleged breach of such information it would not qualify for the narrow exception and would instead be subject to the risk analysis to determine the risk of harm.

There are three exceptions to the definition of “breach” included in the interim final rule, each of which are closely based upon the statutory exceptions to “breach” included in the HITECH Act:

- any unintentional acquisition, access, or use of PHI 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 the HIPAA Privacy Rule
- any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI 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 the HIPAA Privacy Rule
- a disclosure of PHI 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.

In determining whether a breach has occurred, covered entities and business associates will need to (1) determine whether there has been an impermissible use or disclosure of PHI under the HIPAA Privacy Rule, (2) determine and document, through a risk assessment process, whether the impermissible use or disclosure compromises the security and privacy of the PHI, and (3)

determine whether the incident qualifies for any of the regulatory exceptions to the definition of “breach.”

Unsecured PHI

While the definition of “breach” applies to PHI generally, notifications in the event of a breach are only required if there is a breach of “unsecured PHI.” Unsecured PHI is defined as PHI that is not “rendered unusable, unreadable, or indecipherable to unauthorized individuals 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 on the DHHS Web site.”² On April 17, 2009, the DHHS issued guidance on these technologies and methodologies. In response to the comments received, the DHHS has updated that guidance and included it in the interim final rule publication. As in the proposed guidance, encryption and destruction remain the two methods for securing PHI. The body of the updated DHHS guidance,³ which is also available on the DHHS Web site (<http://www.hhs.gov/ocr/privacy>), is included below (footnotes have been omitted):

(a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” 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 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.

(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*.

(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*; 800–77, *Guide to IPsec VPNs*; or 800–113, *Guide to SSL VPNs*, or others which are Federal Information Processing Standards (FIPS) 140–2 validated.

(b) The media on which the PHI is stored or recorded have 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 data destruction.
- (ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

In this updated guidance, the DHHS has clarified that only the destruction of paper PHI, and not redaction, will satisfy the requirements to relieve a covered entity or business associate from breach notification. However, redacted information may not require breach notification either if the information was redacted to the point that it is de-identified, or because it does not pose a significant risk of harm.

Additionally, after reviewing comments received in response to DHHS' solicitation on the topic, the DHHS has concluded that it will not consider limited data sets as a method for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. However, as discussed above, there is a narrow exception for limited data sets in the definition of "breach."

It is important to remember that the guidance addresses PHI and methods and technologies to render PHI unusable, unreadable, or indecipherable to unauthorized individuals. PHI that has been de-identified is no longer PHI and is not subject to the HIPAA Privacy and Security rules. As noted in our prior article on this topic, health care entities, especially business associates, should carefully analyze their need for data to be personally identified and look for ways to properly de-identify PHI so that such data streams are outside regulatory purview. The DHHS is to issue further guidance on de-identification by February 17, 2010.

The DHHS intends the guidance to be an exhaustive list and therefore continues to solicit comments on additional technologies and methodologies to include in future versions of the guidance, which is to be updated annually. Any comments received on the updated guidance will be addressed in the first annual update to the guidance issued in April 2010.

Breach Notification Requirements

Covered entities must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity, to have been accessed, acquired, used or disclosed as a result of a breach. Notice must be made "without unreasonable delay" and not later than 60 days after the discovery of the breach. A breach is treated as discovered as of the first day on which the breach is known to the covered entity, or by exercising reasonable diligence would have been known. Knowledge by a workforce member is imputed to the covered entity. The DHHS emphasizes that the 60 days is an outer limit and that it could be found to be an unreasonable delay to wait until the 60th day to provide notice. There is an exception if law enforcement determines that providing the notice would impede a criminal investigation or cause damage to national security. In the event of a law enforcement exception, the delay is for a length of time requested in writing or for 30 days from an oral request.

Notice of breach should be in plain language and must include:

- a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known
- a description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code)
- the steps an individual should take to protect him/herself from potential harm resulting from the breach
- a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches
- contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, and e-mail address, Web site, or postal address.

Notices should avoid including any sensitive information in the notification itself.

Individual notice may be made by first-class mail or by e-mail if the individual agrees to electronic notice. The notice may be provided in one or more mailings as information becomes available. Telephone notice or notice by other means may be appropriate if urgency is required due to possible imminent

misuse of the information, however this notice is in addition to the required individual notice made by first-class mail or e-mail. The final rule provides for substitute notice in the event there is insufficient or out-of-date contact information that precludes individual notice. If there is insufficient or out-of-date contact information for fewer than ten individuals, then substitute notice can be provided by an alternative form of written notice, telephone or other means. However, if there is insufficient or out-of-date contact information for ten or more individuals then the substitute notice must be in the form of either (1) a conspicuous posting for 90 days on the home page of its Web site, or (2) in major print or broadcast media in geographic areas where individuals affected are likely to reside. Such substitute notice must include a toll-free number (that remains active for at least 90 days) for the individuals to call to find out if their information was included in the breach.

In addition to notices to individuals, for breaches involving more than 500 residents of a state or jurisdiction a covered entity must notify prominent media outlets serving that state or jurisdiction. The media notice must be made without unreasonable delay but not later than 60 calendar days after discovery of the breach. The notice itself must include the same elements included in an individual notice.

Finally, covered entities are required to notify the DHHS. For breaches involving 500 or more individuals, notice is to be made contemporaneously with the notice to individuals and in a manner designated on the DHHS Web site. For breaches involving fewer than 500 individuals, the covered entity shall maintain a log and annually notify the DHHS, no later than 60 days after the end of each calendar year, in the manner provided on the DHHS Web site. In October 2009, the DHHS posted on its Web site the interactive form, together with instructions, for covered entities to notify the DHHS of breaches of unsecured PHI. The same template form⁴ is to be used both for breaches affecting 500 or more individuals and breaches involving fewer than 500 individuals. Additionally, this form is to be used for initial breach reports as well as addenda to prior reports. The requested information on the form includes the type of breach, the location of the breached information, the type of PHI involved as well as the safeguards in place prior to the breach. There is a section for covered entities to inform the DHHS of the type(s) of notice that were taken — individual, substitute and media. Finally, an attestation that the information is accurate is required.

Business associates are required to notify the covered entity of a discovered breach. Such notice is considered discovered on the day the day the breach is known, or by exercising reasonable diligence would have been known, by the business associate. Notice to the covered entity is to be provided without unreasonable delay and in no case later than 60 calendar days after discovery. In instances in which a business associate is acting as the agent of a covered entity, the date of the business associate's discovery of a breach will be imputed to the covered entity and will trigger the 60-day notice period. Covered entities and business associates should address notification timing in their business associate agreements to ensure that any required notifications are made within the required time periods. The business associate's notice to the covered entity must include, to the extent possible, the identification of each affected individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used or disclosed during the breach. The business associate shall also provide the covered entity with any other information that the covered entity is required to provide in its notification to affected individuals.

Preemption

The DHHS received comments regarding issues of preemption and the interaction of the HITECH Act and the DHHS breach notification requirements and state breach notification laws. There already are preemption standards for interaction between HIPAA Privacy and Security Rules and state laws. In general, contrary state law will be preempted by the federal requirements, which serve as a floor; however, if state law is not contrary but provides greater protection to patients, it will be harmonized but not preempted. For example, if a state law requires notification within five days, a covered entity would provide the state-law notice within five days and if there was insufficient information to provide notice as required under the DHHS rule, a second updated notice could be sent within the 60 days required by the DHHS. Similarly, the DHHS regulations include the required minimum content to be included in a breach notification — additional elements required under state law can be included in the same form of notice thereby satisfying both laws. The DHHS is soliciting additional comments on the subject of preemption to allow compliance with applicable state law and the new DHHS regulations.

FINAL FTC BREACH NOTIFICATION RULE

In addition to requiring the DHHS to adopt regulations regarding breach notification for HIPAA-covered entities and their business associates, the HITECH Act requires the FTC to implement regulations on breach notification requirements for vendors of personal health records (PHRs) and certain other non-HIPAA-covered entities. On April 16, 2009, the FTC issued a proposed breach notification rule⁵ and, on August 17, 2009, the FTC issued the final rule.⁶ The FTC final rule on breach notification will go into effect on September 24, 2009. In order to give entities time to come into compliance, the FTC states that it will not bring enforcement actions for breaches that are discovered prior to February 22, 2010.

The HITECH Act also directs the DHHS and the FTC to study and submit by February 17, 2010 a joint report to Congress on privacy and security and breach notification requirements for entities that are not HIPAA-covered entities or business associates, such as PHR vendors and other related entities and service providers. Until Congress enacts any new legislation implementing recommendations included in the DHHS/FTC report, the notification requirements of Section 13407 of the HITECH Act and the FTC final rule provide temporary breach notification requirements enforceable by the FTC.

The FTC's final rule on breach notification responds to points made in the approximately 130 comments received on the proposed rule and includes insight into the FTC's interpretations. In general, the FTC adopted much of the proposed rule with a few significant changes. The remainder of this section of the article will focus on key changes and clarifications made in the FTC's final rule.

The FTC adopts as final the language in the proposed rule that the FTC rule will not apply to HIPAA-covered entities or to business associates engaging in activities as a business associate of a covered entity. However, in response to the many comments received, the FTC included guidance on the application of the FTC rule to HIPAA-covered entities and other dual-role scenarios. The FTC final rule expressly adopts the preemption approach used in HIPAA — contrary state law is preempted by the FTC final rule, however, it should be possible for entities to comply with both federal and state law requirements when providing notifications.

Despite receiving many comments about the rebuttable presumption included in the definition of "breach of security"

IN THE TIME REMAINING BEFORE THE AGENCY ENFORCEMENT DELAYS EXPIRE, ORGANIZATIONS SHOULD NOW FAMILIARIZE THEMSELVES WITH THE DHHS AND FTC BREACH NOTIFICATION REGULATIONS AND DEVELOP BREACH INCIDENT PROGRAMS IN ORDER TO ACHIEVE COMPLIANCE BY MID-FEBRUARY 2010.

— which provides that if there is unauthorized access to an individual's unsecured PHR identifiable health information, unauthorized acquisition will be presumed — the FTC has adopted without modification the rebuttable presumption. The FTC final rule adopts as the definition of "unsecured" information, the DHHS guidance discussed above regarding methodologies and technologies for securing information.

The FTC final rule clarifies that vendors of PHR vendors are to notify their third-party service providers of the vendors' status as PHR vendors, and consequently, the third party's obligations to notify the vendor in the event of a discovery of a breach of security. Additional clarification is provided that a breach will be deemed to have been discovered on the first day the breach of security is known, or reasonably should have been known, by the PHR vendor or related entity or third-party service provider.

The FTC final rule also includes a number of changes regarding breach notification procedures.

- Notices are to be provided in plain language.
- The notice is to describe "what happened" rather than "how the breach occurred." The FTC described concerns raised in comments on the proposed rule that an explanation of how the breach occurred may create unnecessary security risks by providing information potentially providing a roadmap for others attempting to breach security of PHR identifiable information.

- The period for posting conspicuous Web site notice, provided as a substitute for individual notice in those instances where information for ten or more individuals is insufficient or out of date, has been shortened from six months to 90 days.
- There is no specific content requirement for notice to the media, provided in the event of a breach of security involving unsecured PHR identifiable health information involves 500 or more individuals. The wording from the proposed regulation requiring the same content as that provided in individual's notification of breach has been removed in the final rule.
- The period for providing notice to the FTC of breaches involving 500 or more people has been extended from five business days to ten business days following the date of discovery of the breach of security.
- The deadline for submitting the annual log to the FTC of breaches involving information of fewer than 500 individuals now is no later than 60 days after the end of the calendar year (as opposed to 12 months after the date of the first discovered breach, as was described in the proposed rule).
- The FTC has developed a form (attached to the final rule⁷) and to be available on the FTC Web site, for providing notice to the FTC both for prompt notice of breaches involving information of 500 or more individuals, as well as for the annual report of breaches involving information of fewer than 500 individuals.

The FTC has made an effort to have the final breach notification rule align with the DHHS rule where possible under the statutory requirements dictated by the HITECH Act. The FTC addresses its efforts to harmonize various provisions with the DHHS requirements so as to limit the instances in which individuals would receive multiple notifications for the same breach. Whether this has been successful will be better known as the health care industry absorbs and implements the FTC final rule and the DHHS interim final rule.

PRACTICAL APPROACH TO RESPONDING TO BREACH INCIDENTS

What practical steps should organizations take today to be prepared for a breach incident? A breach incident response program begins with a policy establishing management's commitment to the success of the program. This policy will provide the purposes, objectives and the scope of the breach incident response

program. It contains a statement of the key persons within the organization who are responsible for the program.

The breach incident response program can be divided into five distinct phases:

- preparation
- detection
- analysis and prioritization
- containment, investigation and mitigation
- notification
- post-incident activity.

Preparation

An initial step in preparing your incident response program is to create a team that will provide a coordinated and thorough breach incident response. The typical team consists of members inside and outside the organization. Inside members include individuals from a company's legal, information security, privacy, communications, information technology, human resources and compliance departments. Outside members who support the team may include outside counsel, public relations specialists, forensics consultants and law enforcement. The names of the team members and their contact information is included and kept current in the breach incident response procedures so that persons can be quickly contacted when necessary.

Incident response procedures are developed in a manner that includes a clear delineation of the roles, responsibilities and level of authority of team members so that questions on how the team responds do not first arise during the breach incident. Since the nature of breach incidents requires the team members to act swiftly but respond in a flexible manner, effective incident response procedures require a balance between a description of general roles, responsibilities and relationships and specific step-by-step procedures to be followed when a breach occurs.

Training is required to properly prepare for a breach incident. A popular form of training is a tabletop exercise in which the incident response team and other participants respond to a mock breach incident scenario. Training for employees, contractors and business associates is also important so that they can assist in preventing breach incidents and in detecting and reporting potential breach incidents.

Detection, Analysis and Prioritization

Detection

Incidents may be detected through technology and human involvement. The most common type of technologies used to detect incidents are intrusion detection and protection systems, antivirus software and log analyzers.

Employees, contractors and third parties using the organization's information system often detect indicators of incidents in the form of unusual system activity, including sluggish computers and corrupted files. Even though these occurrences may be due to other technical problems, prompt reporting of unusual system activity enhances the breach incident team's ability to analyze and respond to breach incidents when they do occur. A reporting procedure promotes effective information reporting and communication, identifies persons or departments to be contacted, encourages prompt reporting. For smaller organizations, the initial incident report can be accomplished by contacting the help desk, while organizations that are larger may require more formal reporting steps.

Analysis and Prioritization

The detection and reporting of unusual activity does not automatically mean that a breach incident requiring full team response has occurred. Organizations often experience attempted attacks on their systems or other minor incidents that do not warrant any action by the breach incident response team.

To help determine the proper response, breach incident procedures include a categorization of breach incidents, their potential consequences on the organization and appropriate responses. Prioritization of the level of response is based on a predetermined rating of severity of incidents. This permits escalation of the response depending on the severity of the incident.

For compliance with the DHHS and the FTC breach notification regulations, the breach incident classification will also include an analysis of whether a breach, as defined by these rules, has occurred and otherwise warrants notification to affected individuals. This was discussed in detail in this article. However, the analysis should also include a determination of whether any other breach notification rules apply. This includes a determination of whether personal information defined by state breach notification requirements was acquired by an unauthorized person triggering notification regardless of whether the DHHS or FTC rules apply.

Containment, Investigation, and Mitigation

Containment

Containment occurs simultaneously with the determination that a breach incident has been identified as warranting a breach incident team response. Containment is the process of stopping the spread of an incident. Containment decisions are much easier to make if they are considered prior to an incident as part of the breach incident plan. Criteria to consider in determining whether containment is required include:

- potential damage to resources
- need for evidence preservation
- the availability of services needed for containment
- time and resources needed to implement containment strategy
- potential effectiveness of the strategy
- how quickly containment can be achieved.

In cases in which the potential damages are minimal, containment may be delayed to monitor the attacker's activities and to gather additional evidence.

Investigation

Investigation is used to collect evidence as soon as possible after the incident occurs. Investigation can be used to address regulatory violations, determine if a breach of contract occurred, and to support legal proceedings. With regard to compliance with the DHHS and FTC breach notification rules, it can be used to confirm that a breach as defined by those rules has occurred, to determine the PHI that was subject to the breach and to identify the affected individuals.

Investigations should include computer forensics, which is a methodology used to capture volatile information that may not be recorded in a file system or image backup before copying files from the affected host. A computer forensics expert will find the data by looking at network connections and processes, login sessions, open files, file fragments, network interface configurations and the contents of memory. The data may not only be useful to help determine the PHI involved in the breach and the identities of affected persons, they may also provide clues to the identity of the attacker or the attack methods that were used.

Documentation should be kept throughout the investigation, including every step taken from the time the incident was detected to its final resolution.

Since the information can be used as evidence in the court of law or as part of an agency investigation, legal counsel should be involved to ensure that evidence is documented and tagged in a manner that demonstrates that the evidence is safeguarded.

Mitigation

Mitigation is the process to eliminate the causes and results of a breach incident and restoring processes. It includes both technical mitigation and legal mitigation. Technical mitigation involves restoring systems to normal operations and hardening them to prevent similar incidents. This includes deleting malicious code, disabling breached user accounts, restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, changing passwords, and tightening network perimeter security.

Legal mitigation involves the analysis of policies and procedures to determine if any were inadequate in a manner that helped lead to the breach. This includes identification of the persons who were responsible for the breach, redrafting policies and procedures, and providing additional training to employees and business associates.

Notification

Internal Notification

Breach incident procedures identify the persons in the organization who must be notified when a breach incident occurs. This includes persons who are not directly part of the breach incident team but need to be notified to assist in a supporting or managerial role.

External Notification

This article includes detailed analysis of determining whether external notice to the affected individuals is required by the DHHS and FTC rules, the notification content and procedures to be followed when providing notice to affected individuals. However, a breach incident may require notification to persons other than affected individuals.

For example, it may be important to contact law enforcement to assist in the investigations. Notification to a public relations firm may be needed to help with external communications about the incident. It is better to consider these options during the breach

incident response planning phase rather than after an incident occurs. Early consideration of those entities who may be notified when a breach occurs will permit the organization to develop cooperative incident response procedures with external entities and to build good relationships that will benefit the organization when a breach occurs.

Even if PHI is not involved, notification may be required under state law. The analysis to determine whether breach notification is required under state law is similar, but not identical, to that described in this article. Therefore, the incident response procedures should include who should be notified if a breach occurs under state law. This analysis should also include how the breach notification is to be accomplished, including timing, content and method of notice. If applicable, the notification under DHHS and FTC rules should be combined with the notification required by state law.

Post-Incident Activity

After a breach occurs, it is very important to review how the breach was handled so that adjustments may be made to improve the breach incident response program. Post-incident review can be conducted by a special team formed to conduct the review or by internal audit. The review team looks at what occurred, and when and how well the security response team and management performed when dealing with the incident, by looking at whether:

incident policies, procedures and plans were properly followed the incident response tools and internal and external resources were adequate the incident response team model and structure functioned well when responding to the incident the incident handler training and education were adequate the incident documentation and reports were sufficient whether the identified measures of success were met.

Responses to the post-incident review will identify which aspects of the breach incident procedure should be changed and improved. After the breach incident procedures are modified, additional training will be provided to the breach incident team, employees, contractors and business associates to avoid incidents or improve management of future incidents should they occur.

CONCLUSION

In the time remaining before the agency enforcement delays expire, organizations should now familiarize themselves with the DHHS and FTC breach notification regulations and develop breach incident programs in order to achieve compliance by mid-February 2010.

ENDNOTES

- ¹ 74 Fed. Reg. 42740 (August 24, 2009).
- ² 45 C.F.R. § 164.402 at 74 Fed. Reg. 42740, 42768 (August 24, 2009).
- ³ 74 Fed. Reg. 42740, 42742-42743 (August 24, 2009).
- ⁴ The DHHS instructions and form of “Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information,” are available on the DHHS Web site at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.
- ⁵ 74 Fed. Reg. 17914 (April 20, 2009).
- ⁶ 74 Fed. Reg. 42962 (August 25, 2009).
- ⁷ 74 Fed. Reg. 42962, 42983-42985 (August 25, 2009).

RSS on www.pepperlaw.com

SUBSCRIBE TO THE LATEST PEPPER ARTICLES
VIA RSS FEEDS. VISIT WWW.PEPPERLAW.COM
TODAY AND CLICK ON THE RSS BUTTON ON
THE PUBLICATIONS PAGE TO SUBSCRIBE TO
OUR LATEST ARTICLES IN YOUR NEWS READER.
