HIPAA ESSENTIALS

A Guide for Employers

J. J. Keller
& Associates, Inc.®
Since 1953

This publication updates in February/August

19-M (9214)

ISBN 978-1-61099-428-6
90000
9 781610 994286

J. J. Keller & Associates, Inc.
3003 Breezewood Lane
P.O. Box 368
Neenah, Wisconsin 54957-0368
Phone: (800) 327-6868
Fax: (800) 727-7516
JJKeller.com

Library of Congress Catalog Card Number: 2003114412

ISBN 978-1-61099-428-6

Printed in the U.S.A.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes provisions for portability, nondiscrimination, and privacy of individually identifiable health information. These standards created the first-ever national standards to protect the confidentiality of an individual's protected health information (PHI).

The portability and nondiscrimination provisions allow employees to move from one company to another without risking the loss of health care coverage, and prohibit employers from using health status as a reason for denying benefits. These provisions are governed by the Department of Labor's Employee Benefits Security Administration.

Developed by the U.S. Department of Health and Human Services (HHS), the privacy rules provide individuals with access to their medical records, more control over how their PHI is used and disclosed, and the right to examine and obtain a copy of their own health records, and request correction. In addition, it generally limits release of information to the minimum reasonably needed for the purpose of the disclosure. Before the privacy rule took effect, PHI generally could be distributed, without either consent or authorization, for reasons that had nothing to do with an individual's medical treatment or payment.

This manual is designed with group health care plan sponsors in mind, and includes the HIPAA regulations, sample forms, and other documents, along with an index for easier access to information.

Revision bars, like the one at the left of this paragraph, are used in this publication to show where significant changes were made on update pages. They also indicate updates to tables of contents. The revision bar next to text on a page indicates that the text was revised. The date at the bottom of the page tells you when the revised page was issued.

Due to the constantly changing nature of government regulations, it is impossible to guarantee absolute accuracy of the material contained herein. The Publisher and Editors, therefore, cannot assume any responsibility for omissions, errors, misprinting, or ambiguity contained within this publication and shall not be held liable in any degree for any loss or injury caused by such omission, error, misprinting, or ambiguity presented in this publication.

This publication is designed to provide reasonably accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the Publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

The Editors & Publisher
J. J. Keller & Associates, Inc.

Published & Printed by

J. J. Keller & Associates, Inc.
3003 Breezewood Lane, P.O. Box 368
Neenah, Wisconsin 54957-0368
Phone: (800) 327-6868
Fax: (800) 727-7516
JJKeller.com

EDITORIAL

PUBLISHING GROUP

The Editorial Staff is available to provide information generally associated with this publication to a normal and reasonable extent, and at the option of, and as a courtesy of, the Publisher.

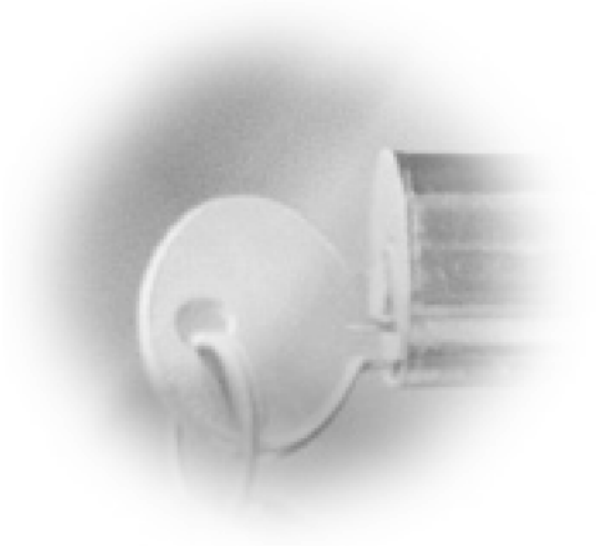


Table of Contents

Privacy

Portability

Reference

Encryption is a method of converting an original message of regular text into encoded or unreadable text that is eventually decrypted into plain comprehensible text.

There are various types of encryption technology available. For an encryption strategy to be successful, you must consider many factors. For example, for encryption technologies to work properly when data is being transmitted, both the sender and the receiver must be using the same or compatible technology.

Organizations use open networks such as the Internet and e-mail systems differently. Currently no single interoperable encryption solution for communicating over open networks exists. Adopting a single industry-wide encryption standard in the security rule would likely have placed too high a financial and technical burden on many organizations. The security rule allows you the flexibility to determine when, with whom, and what method of encryption to use.

You should discuss reasonable and appropriate security measures for the encryption of EPHI during transmission over electronic communications networks with your IT professionals, vendors, business associates, and trading partners.

If you deal with EPHI, you must consider the use of encryption for transmitting it, particularly over the Internet. As business practices and technology change, situations may arise where EPHI being transmitted from you would be at significant risk of being accessed by unauthorized entities. Where risk analysis shows such risk to be significant, you must encrypt those transmissions under the addressable implementation specification for encryption.

You may want to look at how you transmit EPHI and how often.

If your company does engage in such transmissions, here are some steps and questions to get you started in compliance:

1. Identify any possible unauthorized sources that may be able to intercept and/or modify the information. Identify scenarios that may result in modification to the EPHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors).
    - What measures exist to protect EPHI?
    - What measures are planned to protect EPHI?
    - Is there an auditing process in place?
    - Is there assurance that information is not altered during transmission?
    - Are there trained staff members to monitor transmissions?

2. Develop a transmission security policy. Establish a formal (written) set of requirements for transmitting electronic protected health information.
   - Have the requirements been discussed and agreed to by identified key personnel involved in transmitting electronic health information?
   - Has a written policy been developed and communicated to system users?
3. Implement procedures for transmitting electronic health information using hardware/software if needed. Identify methods of transmission that will be used to protect electronic health information; and any tools and techniques that will be used to support the transmission security policy.
   - Is encryption needed to effectively protect the information?
   - Is encryption feasible and cost effective in this environment?
   - Are staff members skilled in the use of encryption?

For example, a benefits office has decided to use the Internet to transmit plan participant data to a support vendor for backup and contingency operations. The transmission of this data should be protected from disclosure. No one who is not authorized to read the file should be able to monitor the transmission and capture the information during its transmission. The benefits office has decided to design and implement a web application, which enforces the use of strong encryption methods to prevent unauthorized disclosure of the data during transmission.

Incident response

With the constant upsurge of security breaches that involve cyber attacks and as required by the HIPAA security rule, you should have security incident response capabilities established. Although effective incident response planning can be a complex task, it should be one of your priorities.

When establishing incident response capabilities, you should consider the following:

Developing incident response policies, plans, and procedures

An incident response policy assists in having a proper, concentrated, and coordinated approach to responding to incidents. The incident response plan should provide a roadmap for implementing your incident response capabilities. The plan should also meet your distinctive requirements that

relate to your mission, sizes, structures, and functions, and identify the necessary resources and management support. Incident response policies and plans should be approved by management and reviewed on an annual basis.

The incident response procedures should be based on the incident response policy and plan. Incident response procedures are outlines of the specific technical processes, tools, techniques, and forms that are utilized not only by the incident response team, but also by staff who need to report an incident. These procedures should include your processes for:

- Preparing for incidents;
- Detecting and analyzing incidents;
- Containing, eradicating and recovering from incidents; and
- Conducting post-incident activities and reviews.

Building relationships and setting up plans for communicating with internal and external parties regarding incidents

Building relationships and lines of communication between the incident response team and other groups, both internal and external, can be challenging. Plan the communication with these groups before an incident occurs.

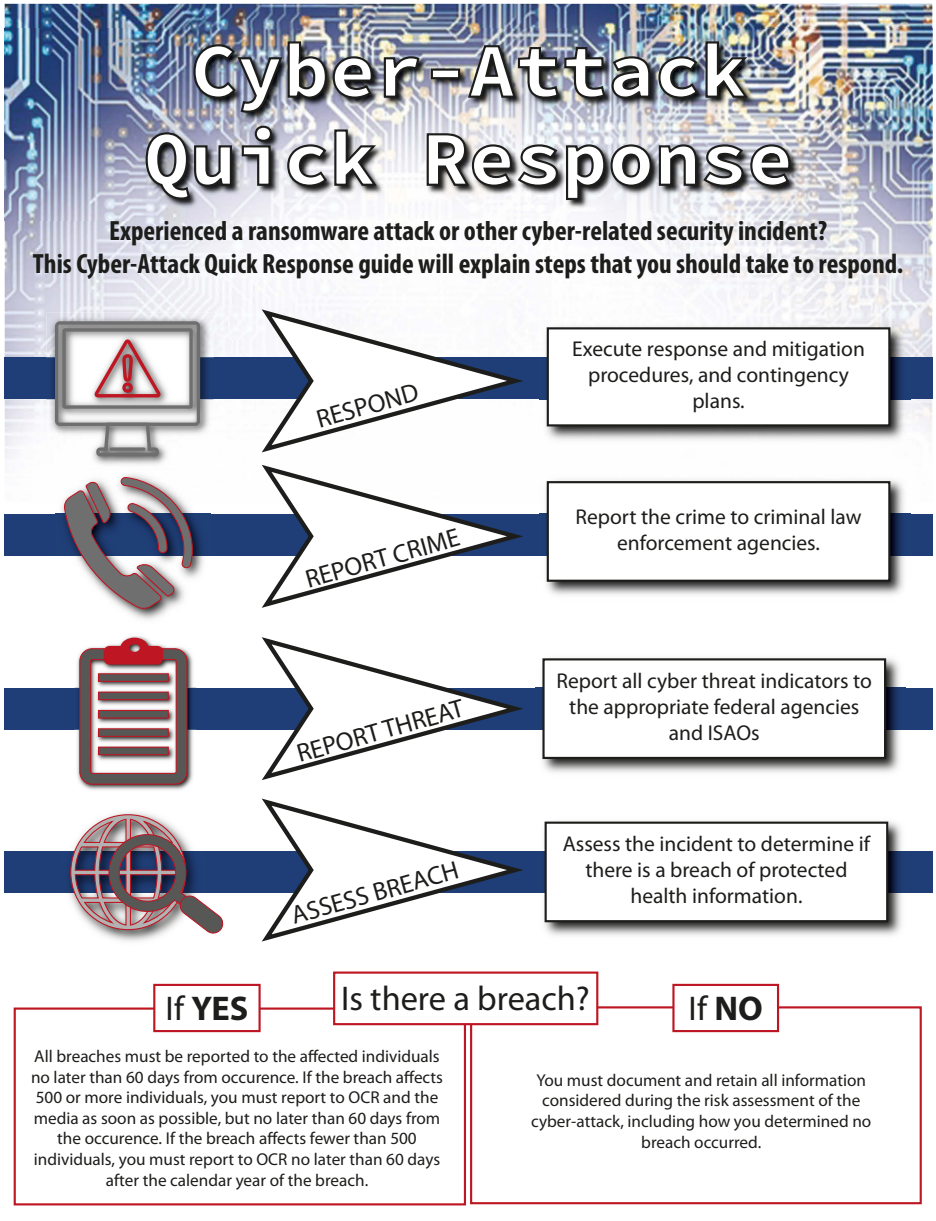
Before establishing incident response policies and procedures, the incident response team should first develop relationships and lines of communication with internal groups within its organization, such as the IT department, public affairs office, legal department, internal law enforcement, and management.

Also, the incident response team should discuss with your public affairs office, legal department, and management about sharing information with external groups. You are often required to communicate with external parties regarding an incident and should comply whenever applicable. External parties could consist of federal agencies, law enforcement, media, internet service providers (ISPs), vendors, or other incident response teams.

Staffing and training

Staff your incident response team with people who have the appropriate skillsets. These skills could include network administration, programming, technical support, intrusion detection, and CyberSecurity forensic analysis; team members should also possess teamwork and communication skills.

Furthermore, incident response team and staff members should be provided with the necessary training to be effective in their roles, and to carry out their responsibilities during an incident or when an incident is suspected.



ISAO = Information-sharing and analysis organizations, such as the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs.

To keep pace with the speed and stealth that cyber adversaries move, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the U.S. Many companies, however, have found it challenging to develop effective information sharing organizations—or ISAOs. In response, President Obama issued the 2015

Executive Order 13691 directing the Department of Homeland Security (DHS) to encourage the development of ISAOs.

In responding to a cyber-attack, for example, you should immediately fix any technical or other problems to stop the incident. You should also take steps to mitigate any impermissible disclosure of PHI, which may be done by your own technology staff, or by an outside vendor brought in to help (the vendor would be a business associate if it has access to PHI for that purpose).

Reporting the crime to other law enforcement agencies may include state or local law enforcement, the FBI, and/or the Secret Service. Any such reports should not include PHI, unless otherwise permitted by the HIPAA privacy rule. If a law enforcement official tells you that any potential breach report would impede a criminal investigation or harm national security, you must delay reporting a breach for the time the law enforcement official requests in writing, or for 30 days, if the request is made orally.

Report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include PHI. OCR does not receive such reports from its federal or HHS partners.

Report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by you at the time of the incident or you determine, through a written risk assessment, that there was a low probability that the information was compromised during the breach. If you discover a breach affecting fewer than 500 individuals, you must notify individuals without unreasonable delay, but no later than 60 days after discovery; and OCR within 60 days after the end of the calendar year in which the breach was discovered.

OCR considers all mitigation efforts taken by you during in any particular breach investigation. Such efforts include voluntary sharing of breach-related information with law enforcement agencies and other federal and analysis organizations as described above.

Cyber extortion

Cyber extortion can take many forms, but it typically involves cyber-criminals' demanding money to stop (or in some cases, to merely delay) their malicious activities, which often include stealing sensitive data or

disrupting computer services. Organizations that provide necessary services or maintain sensitive data are often the targets of cyber extortion attacks.

Ransomware is a form of cyber extortion whereby the attackers deploy malware targeting an organization's data that renderers the data inaccessible, typically by encryption. The encryption key must be obtained from the ransomware attackers to decrypt the data. The ransomware attackers demand payment, often in the form of cryptocurrency (e.g., Bitcoin) for that decryption key. Unfortunately, paying ransom to the attackers may not result in an organization getting its data back. Or, once an organization pays the ransom, the attackers may provide a key to only decrypt a portion of the data and ask for additional ransom to decrypt more data.

Additional examples of cyber extortion include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These types of attacks typically direct such a high volume of network traffic to targeted computers that the affected computers cannot respond and may appear down or otherwise inaccessible to legitimate users. In this type of attack, an attacker may initiate a DoS or DDoS attack against an organization and demand payment to halt the attack, or the attacker could threaten an attack and demand payment to not initiate the attack.

Another type of cyber extortion occurs when an attacker gains access to an organization's computer system, steals sensitive data from the organization, and then threatens to publish that data. The attacker uses the threat of publicly exposing an organization's sensitive data, which could include PHI, to coerce payment. In this type of attack, the attacker already has the organization's data and can sell that data to other malicious persons even after the ransom is paid.

A variation of this type of attack occurs when an attacker steals sensitive data from an organization and then deletes that data from the organization's computers. The attackers then contact the organization informing them that its data has been deleted, but will be returned in exchange for payment. Again, payment of the ransom is no guarantee that an organization will get its data back. In fact, there have been instances where one attacker has stolen and deleted an organization's data while leaving a demand for payment only to have a second attacker gain access to the same computer system and overwrite the payment demand of the first attacker. In this circumstance, the second attacker didn't even have the data, so the organization has no chance of retrieving data from the second attacker.

Although cyber attackers constantly create new versions of malicious software and search for new vulnerabilities to exploit, organizations must continue to be vigilant in their efforts to combat cyber extortion. Examples of activities that might help reduce the chances of being a victim of cyber extortion include:

- Implementing a robust risk analysis and risk management program that identifies and addresses cyber risks holistically, throughout the entire organization;
- Implementing robust inventory and vulnerability identification processes to ensure accuracy and thoroughness of the risk analysis;
- Training employees to better identify suspicious emails and other messaging technologies that could introduce malicious software into the organization;
- Deploying proactive anti-malware solutions to identify and prevent malicious software intrusions;
- Patching systems to fix known vulnerabilities that could be exploited by attackers or malicious software;
- Hardening internal network defenses and limiting internal network access to deny or slow the lateral movement of an attacker and/or propagation of malicious software;
- Implementing and testing robust contingency and disaster recovery plans to ensure the organization is capable and ready to recover from a cyber-attack;
- Encrypting and backing up sensitive data;
- Implementing robust audit logs and reviewing such logs regularly for suspicious activity; and
- Remaining vigilant for new and emerging cyber threats and vulnerabilities (for example, by receiving US-CERT alerts and participating in information sharing organizations.

Ransomware

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015). Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. HIPAA plays a role in assisting to prevent and recover from ransomware attacks, including how HIPAA breach notification processes should be managed in response to a ransomware attack.

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the

hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates (the unauthorized transfer of information from an information system) data, or ransomware in conjunction with other malware that does so.

HIPAA compliance helps covered entities and business associates prevent infections of malware, including ransomware. The HIPAA security rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

- Implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to ePHI and implementing security measures to mitigate or remediate those identified risks;
- Implementing procedures to guard against and detect malicious software;
- Training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and
- Implementing access controls to limit access to ePHI to only those persons or software programs requiring access.

The security management process standard of the security rule includes requirements for all covered entities and business associates to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI created, received, maintained, or transmitted and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level. It is expected that you will use this process of risk analysis and risk management not only to satisfy the specific standards and implementation specifications of the security rule, but also when implementing security measures to reduce the particular risks and vulnerabilities to ePHI throughout your organization's entire enterprise, identified as a result of an accurate and thorough risk analysis, to a reasonable and appropriate level.

For example, although there is a not a security rule standard or implementation specification that specifically and expressly requires you to update the firmware (computer programs and data stored in hardware such that the programs and data cannot be dynamically written or modified during execution of the programs) of network devices, as part of your risk analysis and risk management process, you should, as appropriate, identify and address the risks to ePHI of using networks devices running on obsolete firmware, especially when firmware updates are available to remediate known security vulnerabilities.

In general, moreover, the security rule simply establishes a floor, or minimum requirements, for the security of ePHI; you are permitted (and encouraged) to implement additional and/or more stringent security measures above what is required by security rule standards.

HIPAA compliance also helps recover from infections of malware, including ransomware. The HIPAA security rule requires you to implement policies and procedures that can assist in responding to and recovering from a ransomware attack.

Because ransomware denies access to data, maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack. Test restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities. Because some ransomware variants have been known to remove or otherwise disrupt online backups, you should consider maintaining backups offline and unavailable from your networks.

Implementing a data backup plan is a security rule requirement as part of maintaining an overall contingency plan. Additional activities that must be included as part of your contingency plan include disaster recovery planning, emergency operations planning, analyzing the criticality of applications and data to ensure all necessary applications and data are accounted for, and periodic testing of contingency plans to ensure organizational readiness to execute such plans and provide confidence they will be effective.

During the course of responding to a ransomware attack, you may find it necessary to activate your contingency or business continuity plans. Once activated, you will be able to continue your business operations while continuing to respond to and recover from a ransomware attack. Maintaining confidence in contingency plans and data recovery is critical for effective incident response, whether the incident is a ransomware attack or fire or natural disaster.

Security incident procedures, including procedures for responding to and reporting security incidents, are also required by HIPAA. Your security incident procedures should prepare you to respond to various types of security incidents, including ransomware attacks. Robust security incident procedures for responding to a ransomware attack should include processes to:

- Detect and conduct an initial analysis of the ransomware;
- Contain the impact and propagation of the ransomware;
- Eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- Recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and

- Conduct post-incident activities, which could include a deeper analysis of the evidence to determine if you have any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process to improve incident response effectiveness for future security incidents.

Unless ransomware is detected and propagation halted by your malicious software protection or other security measures, you would typically be alerted to the presence of ransomware only after the ransomware has encrypted the user's data and alerted the user to its presence to demand payment. However, in some cases, your workforce may notice early indications of a ransomware attack that has evaded your security measures.

HIPAA's requirement that your workforce receive appropriate security training, including training for detecting and reporting instances of malicious software, can thus assist you in preparing your staff to detect and respond to ransomware. Indicators of a ransomware attack could include:

- A user's realization that a link that was clicked on, a file attachment opened, or a website visited may have been malicious in nature;
- An increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files);
- An inability to access certain files as the ransomware encrypts, deletes and re-names and/or re-locates data; and
- Detection of suspicious network communications between the ransomware and the attackers' command and control server(s) (this would most likely be detected by IT personnel via an intrusion detection or similar solution).

If you believe that a ransomware attack is underway, either because of indicators similar to those above or other methods of detection, you should immediately activate your security incident response plan, which should include measures to isolate the infected computer systems in order to halt propagation of the attack.

Additionally, it is recommended that if you are infected with ransomware, that you contact your local FBI or United States Secret Service field office. These agencies work with federal, state, local and international partners to pursue cyber criminals globally and assist victims of cybercrime.

You should take some steps if your computer systems are infected with ransomware. The presence of ransomware (or any malware) on your computer systems is a security incident under the HIPAA security rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or

interference with system operations in an information system. Once the ransomware is detected, you must initiate your security incident and response and reporting procedures.

You are required to develop and implement security incident procedures and response and reporting processes that you believe are reasonable and appropriate to respond to malware and other security incidents, including ransomware attacks.

Your security incident response activities should begin with an initial analysis to:

- Determine the scope of the incident to identify what networks, systems, or applications are affected;
- Determine the origination of the incident (who/what/where/when);
- Determine whether the incident is finished, is ongoing or has propagated additional incidents throughout the environment; and
- Determine how the incident occurred (e.g., tools and attack methods used, vulnerabilities exploited).

These initial steps should assist in prioritizing subsequent incident response activities and serve as a foundation for conducting a deeper analysis of the incident and its impact. Subsequent security incident response activities should include steps to:

- Contain the impact and propagation of the ransomware;
- Eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- Recover from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and
- Conduct post-incident activities, which could include a deeper analysis of the evidence to determine if you have any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process to improve incident response effectiveness for future security incidents.

Part of a deeper analysis should involve assessing whether or not there was a breach of PHI as a result of the security incident. The presence of ransomware (or any malware) is a security incident under HIPAA that may also result in an impermissible disclosure of PHI in violation of the privacy rule and a breach, depending on the facts and circumstances of the attack.

If ransomware infects a computer system, the infection could be a HIPAA breach. Whether or not the presence of ransomware would be a breach is a fact-specific determination. A breach under the HIPAA rules is defined as, "…the acquisition, access, use, or disclosure of PHI in a manner not

permitted under the [HIPAA privacy rule] which compromises the security or privacy of the PHI."

When ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA privacy rule.

Unless you can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the breach notification rule, a breach of PHI is presumed to have occurred. You must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements.

You can demonstrate "…that there is a low probability that the PHI has been compromised" such that breach notification would not be required by performing a risk assessment considering at least the following four factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

A thorough and accurate evaluation of the evidence acquired and analyzed as a result of security incident response activities could help with the risk assessment process by revealing, for example: the exact type and variant of malware discovered; the algorithmic steps undertaken by the malware; communications, including exfiltration attempts between the malware and attackers' command and control servers; and whether or not the malware propagated to other systems, potentially affecting additional sources of electronic PHI (ePHI). Correctly identifying the malware involved can help determine what algorithmic steps the malware is programmed to perform. Understanding what a particular strain of malware is programmed to do can help determine how or if a particular malware variant may laterally propagate throughout your enterprise, what types of data the malware is searching for, whether or not the malware may attempt to exfiltrate data, or whether or not the malware deposits hidden malicious software or exploits vulnerabilities to provide future unauthorized access, among other factors.

Although you are required to consider the four factors listed above in conducting risk assessments to determine whether there is a low probability of compromise of the ePHI, you are encouraged to consider

additional factors, as needed, to appropriately evaluate the risk that the PHI has been compromised. If, for example, there is high risk of unavailability of the data, or high risk to the integrity of the data, such additional factors may indicate compromise. In those cases, you must provide notification to individuals without unreasonable delay.

Additionally, with respect to considering the extent to which the risk to PHI has been mitigated (the fourth factor) where ransomware has accessed PHI, you may wish to consider the impact of the ransomware on the integrity of the PHI. Frequently, ransomware, after encrypting the data it was seeking, deletes the original data and leaves only the data in encrypted form. You may be able to show mitigation of the impact of a ransomware attack affecting the integrity of PHI through the implementation of robust contingency plans including disaster recovery and data backup plans. Conducting frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack and ensuring the integrity of PHI affected by ransomware. Test restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities. Integrity to PHI data is only one aspect when considering to what extent the risk to PHI has been mitigated. Additional aspects, including whether or not PHI has been exfiltrated, should also be considered when determining the extent to which the risk to PHI has been mitigated.

The risk assessment to determine whether there is a low probability of compromise of the PHI must be thorough, completed in good faith and reach conclusions that are reasonable given the circumstances. Furthermore, you must maintain supporting documentation sufficient to meet your burden of proof regarding the breach assessment — and if applicable, notification — process including:

- Documentation of the risk assessment demonstrating the conclusions reached;
- Documentation of any exceptions determined to be applicable to the impermissible use or disclosure of the PHI; and
- Documentation demonstrating that all notifications were made, if a determination was made that the impermissible use or disclosure was a reportable breach.

If the ePHI encrypted by the ransomware was already encrypted to comply with HIPAA, a reportable breach might still be involved, as this is a fact-specific determination. The HIPAA breach notification provisions apply to "unsecured PHI," which is PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance. If the ePHI is encrypted in a manner consistent with the guidance such that it is no longer "unsecured PHI," then you are not required to conduct a risk

assessment to determine if there is a low probability of compromise, and breach notification is not required.

However, even if the PHI is encrypted in accordance with the HHS guidance, additional analysis may still be required to ensure that the encryption solution, as implemented, has rendered the affected PHI unreadable, unusable, and indecipherable to unauthorized persons. A full disk encryption solution may render the data on a computer system's hard drive unreadable, unusable, and indecipherable to unauthorized persons while the computer system (such as a laptop) is powered down. Once the computer system is powered on and the operating system is loaded, however, many full disk encryption solutions will transparently decrypt and encrypt files accessed by the user.

For example, if a laptop encrypted with a full disk encryption solution in a manner consistent with HHS guidance is properly shut down and powered off and then lost or stolen, the data on the laptop would be unreadable, unusable, and indecipherable to anyone other than the authenticated user. Because the PHI on the laptop is not "unsecured PHI," you need not perform a risk assessment to determine a low probability of compromise or provide breach notification.

In contrast to the above example, however, if the laptop is powered on and in use by an authenticated user, who then performs an action (clicks on a link to a malicious website, opens an attachment from a phishing email, etc.) that infects the laptop with ransomware, there could be a breach of PHI. If full disk encryption is the only encryption solution in use to protect the PHI and if the ransomware accesses the file containing the PHI, the file containing the PHI will be transparently decrypted by the full disk encryption solution and access permitted with the same access levels granted to the user.

Because the file containing the PHI was decrypted and thus "unsecured PHI" at the point in time that the ransomware accessed the file, an impermissible disclosure of PHI was made and a breach is presumed. Under the HIPAA breach notification rule, notification is required unless you can demonstrate a low probability of compromise of the PHI based on the four-factor risk assessment.

Phishing

Phishing is a type of cyber-attack used to trick individuals into divulging sensitive information via electronic communication by impersonating a trustworthy source. For example, an individual may receive an email or text message informing the individual that their password may have been hacked. The phishing email or text may then instruct the individual to click on a link to reset their password.

In many instances, the link will direct the individual to a website impersonating an organization's real web site (e.g., bank, government agency,

email service, retail site) and ask for the individual's login credentials (username and password).

Once entered into the fake website, the third party that initiated the phishing attack will have the individual's login credentials for that site and can begin other malicious activity such as looking for sensitive information or using the individual's email contact list to send more phishing attacks.

Alternatively, rather than capture login credentials, the link on the phishing message may download malicious software on to the individual's computer. Phishing messages could also include attachments, such as a spreadsheet or document, containing malicious software that executes when such attachments are opened.

Phishing is one of the primary methods used to distribute malicious software, including ransomware.

Individuals must remain vigilant in their efforts to detect and not fall prey to phishing attacks because these attacks are becoming more sophisticated and harder to detect. Phishing attacks take advantage of popular holidays by impersonating messages from shipping vendors and ecommerce sites. Similarly, phishing attacks regarding tax refunds are common during tax season (March and April).

A specific type of phishing attack, known as spear phishing, targets specific individuals within an organization. For example, a spear phishing attack could target an individual in the IT, accounting, or finance department of an organization by impersonating the individual's supervisor and directing the individual to a malicious website or to download a file containing a malicious program. One of the primary methods of combating phishing attacks of all kinds is through user awareness.

Tips to avoid becoming a victim of a phishing attack include:

- Be wary of unsolicited third-party messages seeking information. If you are suspicious of an unsolicited message, call the business or person that sent the message to verify that they sent it and that the request is legitimate.
- Be wary of messages even from recognized sources. Messages from coworkers or a supervisor as well as messages from close relatives or friends could be sent from hacked accounts used to send phishing messages.
- Be cautious when responding to messages sent by third parties. Contact information listed in phishing messages such as email addresses, web sites, and phone numbers could redirect you to the malicious party that sent the phishing message. When verifying the contents of a message, use known good contact information or, for a business, the contact information provided on its web site.

- Be wary of clicking on links or downloading attachments from unsolicited messages. Phishing messages could include links directing people to malicious web sites or attachments that execute malicious software when opened.
- Be wary of even official looking messages and links. Phishing messages may direct you to fake web sites mimicking real websites using web site names that appear to be official, but which may contain intentional typos to trick individuals. For example, a phishing attack may direct someone to a fake website that uses 1's (ones) instead of l's (i.e., a11phishes vs. allphishes).
- Use multifactor authentication. Multifactor authentication reduces the possibility that someone can hack into your account using only your password.
- Keep antimalware software and system patches up to date. If you do fall for a phishing scam, antimalware software can help prevent infection by a virus or other malicious software. Also, ensuring patches are up to date reduces the possibility that malicious software could exploit known vulnerabilities of your computer's or mobile device's operating system and applications.
- Back up your data. In the event that malicious software, such as ransomware, does get installed on your computer, you want to make sure you have a current backup of your data. Malicious software that deletes your data or holds it for ransom may not be retrievable. Robust, frequent backups may be the only way to restore data in the event of a successful attack. Also, be sure to test backups by restoring data from time to time to ensure that the backup strategy you have in place is effective.

Telework and security

Many people telework, which is the ability for an organization's employees and contractors to conduct work from locations other than the organization's facilities. Teleworkers use various devices, such as desktop and laptop computers, cell phones, and personal digital assistants (PDAs), to read and send email, access Web sites, review and edit documents, and perform many other tasks. Most teleworkers use remote access, which is the ability of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities. Organizations have many options for providing remote access, including virtual private networks, remote system control, and individual application access (e.g., Web-based email).

Before allowing telework, ensure that users understand your organization's policies and requirements.

Remind teleworkers of the organization's policies and requirements to help provide adequate security to protect the organization's information. Sensitive information stored on, or sent to or from, external telework devices needs to be protected so that malicious parties can neither access nor alter it. An unauthorized release of sensitive information could damage the public's trust in an organization, jeopardize the mission of an organization, or harm individuals if their personal information has been released.

Make sure all teleworkers' devices on their wired and wireless home networks are properly secured, as well as the home networks themselves.

An important part of telework and remote access security is applying security measures to the personal computers (PCs) and consumer devices using the same wired and wireless home networks to which the telework device normally connects. If any of these other devices become infected with malware or are otherwise compromised, they could attack the telework device or eavesdrop on its communications. Teleworkers should also be cautious about allowing others to place devices on the teleworkers' home networks, in case one of these devices is compromised. This may be something to address in telework policies.

You may want to apply security measures to home networks to which teleworkers' devices normally connect. One example of a security measure is using a broadband router or firewall appliance to prevent computers outside the home network from initiating communications with telework devices on the home network. Another example is ensuring that sensitive information transmitted over a wireless home network is adequately protected through strong encryption.

Consider the security state of a third-party device before using it for telework.

Teleworkers often want to perform remote access from third-party devices, such as checking email from a kiosk computer at a conference. However, teleworkers typically do not know if such devices have been secured properly or if they have been compromised. Consequently, a teleworker could use a third-party device infected with malware that steals information from users (e.g., passwords or email messages).

Many organizations either forbid third-party devices to be used for remote access or permit only limited use, such as for Web-based email. Teleworkers should consider who is responsible for securing a third-party device and who can access the device before deciding whether or not to use it. Whenever possible, teleworkers should not use publicly accessible third-party devices for telework, and teleworkers should avoid using

anythird-party devices for performing sensitive functions or accessing sensitive information.

Secure a telework PC.

If you have teleworkers who use their own desktop or laptop PCs for telework, their operating systems and primary applications should be secured.

- Use a combination of security software, such as antivirus and antispyware software, personal firewalls, spam and Web content filtering, and popup blocking, to stop most attacks, particularly malware;
- Restrict who can use the PC by having a separate standard user account for each person, assigning a password to each user account, using the standard user accounts for daily use, and protecting user sessions from unauthorized physical access;
- Ensure that updates and patches are regularly applied to the operating system and primary applications, such as Web browsers, email clients, instant messaging clients, and security software;
- Disable unneeded networking features on the PC and configure wireless networking securely;
- Configure primary applications to filter content and stop other activity that is likely to be malicious;
- Install and use only known and trusted software;
- Configure remote access software based on the organization's requirements and recommendations; and
- Maintain the PC's security on an ongoing basis, such as changing passwords regularly and checking the status of security software periodically.

Secure consumer devices used for telework.

A wide variety of consumer devices exists, such as cell phones, PDAs, and video game systems, and security features available for these devices also vary widely. Some devices offer only a few basic features, whereas others offer sophisticated features similar to those offered by PCs. This does not necessarily imply that more security features are better; in fact, many devices offer more security features because the capabilities they provide (e.g., wireless networking, instant messaging) make them more susceptible to attack than devices without these capabilities. General recommendations for securing telework devices are as follows:

- Limit access to the device, such as setting a personal identification number (PIN) or password and automatically locking a device after an idle period;
- Disable networking capabilities, such as Bluetooth, except when they are needed;

- Use additional security software, such as antivirus software and personal firewalls, if appropriate;
- Ensure that security updates, if available, are acquired and installed at least monthly, or more frequently; and
- Configure applications to support security (e.g., blocking activity that is likely to be malicious).

Secure information.

Since the information is the focus of privacy and security measures, it is beneficial to look at ways in which it can be at risk of access from unwanted sources and how to minimize those risks.

- Use physical security controls for telework devices and removable media. For example, you might require that laptops be physically secured using cable locks when used in hotels, conferences, and other locations where third parties could easily gain physical access to the devices. You may also have physical security requirements for papers and other non-computer media that contain sensitive information and are taken outside the organization's facilities.
- Encrypt files stored on telework devices and removable media such as CDs and flash drives. This prevents attackers from readily gaining access to information in the files. Many options exist for protecting files, including encrypting individual files or folders, volumes, and hard drives. Generally, using an encryption method to protect files also requires the use of an authentication mechanism (e.g., password) to decrypt the files when needed.
- Ensure that information stored on telework devices is backed up. If something adverse happens to a device, such as a hardware, software, or power failure or a natural disaster, the information on the device will be lost unless it has been backed up to another device or removable media. Some organizations permit teleworkers to back up their local files to a centralized system (e.g., through VPN remote access), whereas other organizations recommend that their teleworkers perform local backups (e.g., burning CDs, copying files onto removable media). Teleworkers should perform backups, following your organizations' guidelines, and verify that the backups are valid and complete. It is important that backups on removable media be secured at least as well as the device that they backed up. For example, if a computer is stored in a locked room, then the media also should be in a secured location; if a computer stores its data encrypted, then the backups of that data should also be encrypted.
- Ensure that information is destroyed when it is no longer needed. For example, files should be removed from a computer scheduled to be retired or from a third-party computer that is temporarily used for

remote access. Some remote access methods perform basic information cleanup, such as clearing Web browser caches that might inadvertently hold sensitive information, but more extensive cleanup typically requires using a special utility, such as a disk-scrubbing program specifically designed to remove all traces of information from a device. Another example of information destruction is shredding telework papers containing sensitive information once the papers are no longer needed.

- Erase information from missing cell phones and PDAs. If a cell phone or PDA is lost or stolen, occasionally its contents can be erased remotely. This prevents an attacker from obtaining any information from the device. The availability of this service depends on the capabilities of the product and the company providing network services for the product.

Forgetting the importance of safeguarding Internet-accessible PHI can be a costly mistake for a covered entity. A health care provider found this out the hard way when it settled with the U.S. Department of Health and Human Services (HHS) for $100,000.

The entity, a provider of surgery physician services, reportedly posted clinical and surgical appointments for its patients on a publicly accessible Internet-based calendar. A report detailing this practice caught the eye of the HHS, which investigated. The investigation found the health care provider had implemented few policies and procedures to comply with the HIPAA privacy and security rules, and had limited safeguards in place to protect patients' electronic protected health information (EPHI), according to the HHS.

In addition to posting PHI on a public Internet-based calendar, the provider reportedly also made the following mistakes:

- Transmitted EPHI from a company Internet-based email account to employees' personal Internet-based email accounts on a daily basis for four years;
- Failed to identify a security official;
- Failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of patient EPHI; and
- Failed to obtain business associate agreements from the Internet-based calendar and email provider certifying that these entities would appropriately safeguard the EPHI received from the health care provider.

In addition to paying the $100,000 in the settlement, the health care provider entered into a corrective action plan with the HHS.

Adequately protect remote access-specific authenticators.

Teleworkers need to ensure that they adequately protect their remote access-specific authenticators, such as passwords, personal identification numbers (PINs), and hardware tokens. Such authenticators should not be stored with the telework computer, nor should multiple authenticators be stored with each other (e.g., a password or PIN should not be written on the back of a hardware token).

Beware social engineering.

Teleworkers should be aware of how to handle threats involving social engineering, which is a general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. For example, an attacker might approach a teleworker in a coffee shop and ask to use the computer for a minute or offer to help the teleworker with using the computer.

Teleworkers should also be wary of any requests they receive that could lead to a security breach or to the theft of a telework device.

Know how to handle a security breach.

If a teleworker suspects that a security breach (including loss or theft of materials) has occurred involving a telework device, remote access communications, removable media, or other telework components, the teleworker should immediately follow your organization's policy and procedures for reporting the possible breach. This is particularly important if any of the affected telework components contain sensitive information such as EPHI, so that the potential impact of a security breach is minimized.

For more information on breaches, see the Protected Health Information chapter.

Mobile technology

There have been a number of security incidents related to the use of laptops, other portable and/or mobile devices, and external hardware that store, contain, or are used to access electronic protected health information (EPHI) under the responsibility of a HIPAA-covered entity. All covered entities are required to be in compliance with the HIPAA security rule, which includes, among its requirements, reviewing and modifying, where necessary, security policies and procedures on a regular basis. This is particularly relevant for organizations that allow remote access to EPHI through portable devices or on external systems or hardware not owned or managed by the covered entity.

The main objective of this information is to reinforce some of the ways you may protect EPHI when it is accessed or used outside of your organization's physical purview. It sets forth strategies that may be reasonable and appropriate for your organization if you conduct some of your business activities through:

1. The use of portable media/devices (such as USB flash drives) that store EPHI; and
2. Offsite access or transport of EPHI via laptops, personal digital assistants (PDAs), home computers, or other noncorporate equipment.

The Centers for Medicare & Medicaid Services (CMS) has delegated authority to enforce the HIPAA security standards, and may rely upon this information in determining whether or not the actions of a covered entity are reasonable and appropriate for safeguarding the confidentiality, integrity, and availability of EPHI, and it may be given deference in any administrative hearing pursuant to the HIPAA enforcement rule.

The kinds of devices and tools about which there is growing concern because of their vulnerability include the following examples: laptops; home-based personal computers; PDAs and smartphones; hotel, library, or other public workstations and wireless access points (WAPs); USB flash drives and memory cards; floppy disks; CDs; DVDs; backup media; email; smart cards; and remote access devices (including security hardware).

Managing mobile devices

If members of your plan workforce might be using mobile devices in their work, the plan must comply with the HIPAA privacy and security rules to protect and secure health information, even when using mobile devices. Therefore, you are to develop and implement mobile device procedures and policies that will protect PHI. Here are some steps to consider.

1. Decide whether mobile devices will be used to access, receive, transmit, or store protected health information or used as part of your organization's internal networks or systems.

   Understand the risks to your organization before you decide to allow the use of mobile devices. Risks (threats and vulnerabilities) can vary based on the mobile device and its use. Some risks might include:

   - A lost mobile device;
   - A stolen mobile device;
   - Inadvertently downloading viruses or other malware;
   - Unintentional disclosure to unauthorized users when sharing mobile devices with friends, family, and/or coworkers; or
   - Using an unsecured Wi-Fi network.

J. J. Keller & Associates, Inc.®
Since 1953

Want to Keep Reading?

Visit JJKeller.com now to order or get more details on this manual written by our safety & compliance experts.

Convenient Update Service subscriptions are also available to help you make sure your information is always up to date.

NOW AVAILABLE - Access Your Manual Online

With our NEW Online Edition options, you can access this manual's content from any browser or mobile device. You'll get:

- Search capabilities for easy navigation and fast research
- Bookmarks to help you to quickly flip to sections you frequently use
- Continuous updates to ensure you always have the most current info
- Notifications via homepage and email to help you stay on top of changes
- Easy access to ask questions of our subject matter experts

Order Now to Keep Reading!

Connect With Us

@jjkeller | jjkeller.com/LinkedIn | google.com/+jjkeller | contact us