U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

FACT SHEET: Ransomware and HIPAA

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).[1] 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. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

1. What is ransomware?

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[2] data, or ransomware in conjunction with other malware that does so.

2. Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?

Yes. 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 electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- implementing procedures to guard against and detect malicious software;

---

[1] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware* available at https://www.justice.gov/criminal-ccips/file/872771/download.

[2] Exfiltration is "[t]he unauthorized transfer of information from an information system." NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. (April 2013). Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

- 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 the entities create, receive, maintain, or transmit and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level. It is expected that covered entities and business associates 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 an 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 entities to update the firmware[3] of network devices, entities, as part of their risk analysis and risk management process, 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; entities are permitted (and encouraged) to implement additional and/or more stringent security measures above what they determine to be required by Security Rule standards.

3. Can HIPAA compliance help covered entities and business associates recover from infections of malware, including ransomware?

Yes. The HIPAA Security Rule requires covered entities and business associates to implement policies and procedures that can assist an entity 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, entities should consider maintaining backups offline and unavailable from their networks.

[3] Firmware refers to "[c]omputer programs and data stored in hardware… such that the programs and data cannot be dynamically written or modified during execution of the programs." NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. (April 2013).
Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Implementing a data backup plan is a Security Rule requirement for HIPAA covered entities and business associates as part of maintaining an overall contingency plan. Additional activities that must be included as part of an entity's 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. See 45 C.F.R. 164.308(a)(7).

During the course of responding to a ransomware attack, an entity may find it necessary to activate its contingency or business continuity plans. Once activated, an entity will be able to continue its 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. See 45 C.F.R. 164.308(a)(6). An entity's security incident procedures should prepare it 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[4]:

- 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 the entity has 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 of the entity to improve incident response effectiveness for future security incidents.

4. How can covered entities or business associates detect if their computer systems are infected with ransomware?

Unless ransomware is detected and propagation halted by an entity's malicious software protection or other security measures, an entity 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, an entity's workforce may notice early indications of a ransomware attack that has evaded the entity's security measures. HIPAA's requirement that an entity's workforce receive appropriate security training, including training for detecting and reporting instances of malicious

[4] Adapted from NIST SP 800-61Rev. 2, *Computer Security Incident Handling Guide.*

software, can thus assist entities in preparing their 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 an entity believes that a ransomware attack is underway, either because of indicators similar to those above or other methods of detection, the entity should immediately activate its 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 an entity infected with ransomware contact its 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.

5. What should covered entities or business associates do if their computer systems are infected with ransomware?

The presence of ransomware (or any malware) on a covered entity's or business associate's 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. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R. 164.308(a)(6).

HIPAA covered entities and business associates are required to develop and implement security incident procedures and response and reporting processes that they believe are reasonable and appropriate to respond to malware and other security incidents, including ransomware attacks. Entities seeking guidance regarding the implementation of security incident procedures may wish to review NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide*[5] for additional information.

An entity's security incident response activities should begin with an initial analysis to:

[5] Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- 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 the entity 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 the entity has 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 of the entity 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. See the definition of disclosure at 45 C.F.R. 160.103 and the definition of breach at 45 C.F.R. 164.402.

6. Is it a HIPAA breach if ransomware infects a covered entity's or business associate's computer system?

Whether or not the presence of ransomware would be a breach under the HIPAA Rules 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." See 45 C.F.R. 164.402.[6]

When electronic protected health information (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

[6] See also Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.

Unless the covered entity or business associate 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. The entity 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. See 45 C.F.R. 164.400-414.

7. How can covered entities or business associates demonstrate "…that there is a low probability that the PHI has been compromised" such that breach notification would not be required?

To demonstrate that there is a low probability that the protected health information (PHI) has been compromised because of a breach, a risk assessment considering at least the following four factors (see 45 C.F.R. 164.402(2)) must be conducted:

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 entities with the risk assessment process above 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 assist an entity to 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 an entity's 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 entities are required to consider the four factors listed above in conducting their risk assessments to determine whether there is a low probability of compromise of the ePHI, entities 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, entities must provide notification to individuals without unreasonable delay, particularly given that any delay may impact healthcare service and patient safety.

Additionally, with respect to considering the extent to which the risk to PHI has been mitigated (the fourth factor) where ransomware has accessed PHI, the entity 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. An entity 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, in accordance with 45 C.F.R. 164.530(j)(iv)), covered entities and business associates must maintain supporting documentation sufficient to meet their burden of proof (see 45 C.F.R. 164.414) 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 (see 45 C.F.R. 164.402(1)) 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.

8. Is it a reportable breach if the ePHI encrypted by the ransomware was already encrypted to comply with HIPAA?

This is a fact specific determination. The HIPAA breach notification provisions apply to "unsecured PHI" (see 45 C.F.R. 164.402), which is protected health information (PHI) that is not secured through the use of a technology or methodology specified by the Secretary in guidance. If the electronic PHI (ePHI) is encrypted by the entity in a manner consistent with the *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*[7] such that it is no longer "unsecured PHI," then the entity is not required to conduct a risk assessment to determine if there is a low probability of compromise, and breach notification is not required.

[7] Available at http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

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[8] 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", a covered entity or business associate need not perform a risk assessment to determine a low probability of compromise or provide breach notification.

However, in contrast to the above example, 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 in accordance with 45 CFR 164.404 is required unless the entity can demonstrate a low probability of compromise of the PHI based on the four factor risk assessment (see 45 C.F.R. 164.402(2)).

[8] HHS guidance to render unsecured PHI unusable, unreadable or indecipherable to unauthorized individuals indicates that encryption solutions for data-at-rest must be consistent with NISP SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, in order for encrypted PHI to not be "unsecured PHI". It must be noted, however, that consistency with NIST SP 800-111 requires not only the consideration of an encryption algorithm, but also consideration of additional areas of an encryption solution including encryption methodologies (e.g., full disk, virtual disk/volume, folder/file), cryptographic key management, and pre-boot authentication, where applicable.