PUBLICATION

Ransomware Attack is a Breach – Unless You Can Prove Otherwise

Authors: Samuel Lanier Felker
July 14, 2016

Ransomware is the fastest growing malware threat in the United States, targeting simple home computers to elaborate corporate IT networks. The Federal Bureau of Investigation recently reported an increase in ransomware attacks – more than 4,000 ransomware attacks daily in 2016, which is a 300 percent increase over attacks in 2015. This cyber drama has played out with several high-visibility ransomware attacks on hospitals, substantially threatening their reputations and ability to conduct business.

Recognizing the threat that ransomware poses to our country's critical health care infrastructure, Secretary of Health and Human Services Sylvia M. Burwell recently released a new Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule Guidance on preventing and responding to ransomware attacks, which can be accessed here.

The new Guidance reinforces the need for HIPAA Privacy and Security Rule and Breach Notification Rule policies and procedures to assist organizations in preventing, detecting, containing and responding to ransomware threats. Further, the Guidance created a bright line test for ransomware breaches – highlighting the responsibility of HIPAA covered entities and their business associates to treat the presence of ransomware as a patient and government notifiable event, unless able to prove in writing that no breach of unsecure protected health information (PHI) actually occurred.

Here are some important questions addressed by the HHS/OCR Guidance:

1. If ransomware encrypts unsecure PHI, is patient and governmental notice required?

The most important piece of information that came from the HHS/OCR Guidance is the concept that when unsecured PHI is attacked and encrypted as the result of ransomware, a notifiable breach of unsecured PHI is assumed to have occurred because the unsecure PHI encrypted by the ransomware was in fact acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus, the attack is a "disclosure" of PHI that is not permitted under the HIPAA Privacy Rule. According to the Guidance, unless the covered entity or business associate can prove that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule (and two additional factors provided in the Guidance), a breach of unsecure PHI is presumed to have occurred. The covered entity must then comply with the applicable breach notification provisions, including notification without unreasonable delay of affected individuals, of the Secretary of HHS and of the media (for breaches affecting more than 500 individuals) in accordance with Breach Notification Rule.

To demonstrate that no breach of unsecured PHI occurred because there is a low probability that unsecured PHI has been compromised, a risk assessment considering at least the following factors must be conducted (and maintained in writing) in accordance with the Breach Notification Rule:

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;
4. the extent to which the risk to the PHI has been mitigated;
5. whether there is a high risk of unavailability of PHI; and
6. whether there is a high risk to the integrity of the PHI.

The last two factors noted above are provided in the Guidance and are new to the risk assessment analysis.

The Guidance notes that a thorough and accurate evaluation of the evidence acquired and analyzed as a result of security incident response activities can assist entities 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. Correctly identifying the malware involved can assist an entity in determining 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 hides malicious software or exploits vulnerabilities to provide future unauthorized access, among other considerations.

The Guidance instructs covered entities and business associates to maintain supporting documentation sufficient to meet their burden of proof regarding the breach risk assessment – and if applicable, notification process. In light of pending OCR Phase 2 Audits (see, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html), this documentation will be key to a successful audit. As such, we recommend covered entities and their business associates conduct a full risk assessment to determine whether a breach of unsecured PHI occurred for each security incident, which likely will require the affected entity to obtain a forensic examination of any successful ransomware incident.

2. Is it a reportable breach if the PHI encrypted by the ransomware was already encrypted to comply with the HIPAA Breach Notification Safe Harbor?

The Guidance also tackles the thorny question of whether there is a breach of unsecured PHI when the PHI that is affected by the ransomware was at the time of the attack encrypted in a manner consistent with the safe harbor *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable or Indecipherable to Unauthorized Individuals*. The short answer: this is a fact specific determination. Although the Guidance first states encrypted data that is attacked may not even require a full risk assessment, the Guidance then contradicts itself and warns that, even if the PHI is encrypted, additional analysis may still be required to ensure that the encryption solution, as implemented, has rendered the affected PHI truly unreadable, unusable and indecipherable to the unauthorized person. As such, we recommend covered entities and their business associates who are attacked by ransomware conduct a full risk assessment to determine whether a breach of unsecured PHI occurred, which may involve obtaining a forensic examination of the incident.

3. What should covered entities do if their computer systems are infected with ransomware?

The Guidance recommends that an entity infected with ransomware contact its local FBI or United States Secret Service field office. We have found that notifying law enforcement may allow the law enforcement exception to the Breach Notification Rule to be invoked – allowing more time for investigation and notification, if needed.

On the subject of whether to pay the ransom, the Guidance refers to a recently released U.S. Government interagency technical report entitled "How to Protect Your Networks from Ransomware," which encourages business *not* to pay the ransom, warning there are serious risks to consider:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after paying ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying ransom could inadvertently encourage this criminal business model to continue.

The Guidance also describes in detail the thorough analysis that an attacked entity or business associate should conduct. The initial analysis should:

- 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).
- contain the impact and propagation of the ransomware; and
- eradicate the instances of ransomware.

The job isn't done once the attack is thwarted. Important next steps noted in the Guidance include:

- the entity must mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation in the first place;
- 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 HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?

The HIPAA Security Rule clearly requires the implementation of security measures that can help prevent the introduction of malware, including ransomware. The Guidance reminds entities that those required security measures that are particularly useful for combating ransomware include:

- conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information;
- 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 electronic protected health information (PHI) to only persons or software programs requiring access.

The Guidance emphasizes that covered entities and business associates are expected to use the 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 electronic PHI throughout an organization's entire enterprise. For example, although there is a not a Security Rule standard or implementation specification that specifically and expressly requires entities to update the firmware of network devices as part of their risk analysis and risk management process, entities should, as appropriate, identify and address the risks to electronic PHI of using networks devices running on obsolete firmware, especially when firmware updates are available to remediate known security vulnerabilities. In other words, the Security Rule simply establishes a floor, or minimum requirements, for the security of electronic PHI, and HIPAA covered entities and their business associates are encouraged to implement additional and/or more stringent security measures above those required by the Security Rule.

5. How can HIPAA compliance help covered entities and business associates recover from ransomware infections?

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. Implementing a data backup plan is a well-known and established Security Rule requirement for HIPAA covered entities and business associates as part of maintaining an overall contingency plan. The Guidance reminds entities that 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. To verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities, testing of restoration systems should be periodically conducted. Further, because some ransomware variants have been known to remove or otherwise disrupt online backups, the Guidance recommends entities consider maintaining backups offline and unavailable from their networks.

Security incident procedures, including procedures for responding to and reporting security incidents, are also well-known and established requirements of HIPAA. According to the Guidance, an entity's security incident procedures should prepare it to respond to ransomware attacks, including 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 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.

We recommend our clients engage HIPAA attorneys, forensic and breach notification consultants as part of their compliance response plans to ensure these professionals are ready, willing and legally required to assist timely in the event of a breach.

In the event of a ransomware attack or for assistance with your HIPAA Privacy, Security and Breach Response and Notification policies and procedures, do not hesitate to contact Samuel L. Felker, CIPP/US or one of the other members of our Privacy and Security Team.