Ransomware and Healthcare Providers

Zachary Steadman
zsteadman@mwlaw.com
(501) 688.8892

06/13/2017

On February 5, 2016, hackers hijacked Hollywood Presbyterian Medical Center's computer systems using ransomware that infects via email and locks a victim's computer, core server or even its backup repositories and prevents access to data.[i] Typically, ransomware encrypts the files and creates a key stored on the malware control servers and sends a message offering to decrypt the data if a ransom payment, usually in bitcoin, is made by a stated deadline.[ii] This offer often coincides with a threat to delete the key if the deadline passes without payment. If a deadline is not met, the malware's operators may offer to decrypt the data via an online service for a significantly higher price in bitcoin. The Hollywood Presbyterian hacker demanded the equivalent of $17,000 in bitcoin currency to unlock the systems, leading to a two-week standoff that ended when the hospital paid the ransom prior to engaging law enforcement.[iii]

Since the Hollywood Presbyterian incident, hackers have compromised the computer systems of three other hospitals in southern California: Chino Valley Medical Center, a 126-bed community hospital in Chino; Desert Valley Hospital, a 148-bed acute care facility in Victorville; and Alvarado Hospital Medical Center, a 306-bed hospital in San Diego. However, California is not the only state in which hospitals are being targeted. King's Daughters' Health in southeast Indiana discovered a single employee's file had been infected with a ransomware virus.[iv] Methodist Hospital in Henderson, Kentucky, fell victim to a ransomware attack via spam email regarding invoices and opening an attached file.[v] Possible ransomware attacks infected the systems at Ruby Memorial Hospital in West Virginia, causing the security cameras offline and the hospital to go on lockdown for approximately four hours[vi] and MedStar Health, an operator of ten hospitals and 250 out-patient clinics in the Maryland and Washington, DC area, locking its users out of its system and resulting in shutting down large portions of its network.[vii] Hackers took a step further in an attack against Kansas Heart Hospital by demanding a second ransom to decrypt hostage data after the hospital paid the first ransom.[viii]

Thus far, these recent ransomware attacks have not resulted in a compromise to patient information, as hackers are merely looking to make easy money with low risk.[ix] Regardless, ransomware attacks pose a real and tangible threat to the healthcare industry. According to FBI estimates, the CryptoLocker strain of ransomware resulted in a $27 million pay out in six months during 2014.[x] More recently, the ransomware known as Locky has been used in several of the attacks referenced here. According to Wired.com, Locky delivers a mass email with the hope that recipients will click and become infected with the ransomware, which ultimately accesses core systems and shared file servers and erases backup files.[xi]

Although hospitals are not the only targets for these attacks[xii], they are probable targets because of their increased use of new medical devices, staff and use of multiple operating systems.[xiii] Most of the attacks referenced here have not yet resulted in ransom payments, but some suggest the targeting of hospitals is a result of the publicity of the Hollywood Presbyterian ransom payment.[xiv]

The rise in ransomware attacks has created an interesting question as to whether or not the attack qualifies as a security incident or a reportable breach as defined by the Health Insurance Portability and Accountability Act ("HIPAA"). If a ransomware attack qualifies as a HIPAA breach, the healthcare provider would have to fulfill a number of mitigation and reporting obligations. This analysis applies to business associates who also suffer a breach. In other words, if a law firm, accounting firm or other vendor acting as a business associate falls victim to a ransomware attack, that business or individual may need to fulfill the same mitigation and reporting obligations. The remainder of this article discusses HIPAA security incident and breach requirements when dealing with ransomware attacks. The article discusses affected entities in terms of healthcare providers. However, the relevant analysis may apply in situations where a law firm or other business vendor is acting as a business associate. The U.S. Department of Health and Human Services ("HHS") has recognized the impact of ransomware attacks on the healthcare community and has provided new guidance on ransomware that is also discussed below.

Security Incident

The first issue is whether or not the ransomware attack qualifies as a security incident. HIPAA requires a healthcare provider to implement policies and procedures to address security incidents. Specifically, a healthcare provider must identify and respond to "suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the healthcare provider; and document security incidents and their outcomes."[xv] A security incident is broadly defined as an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.[xvi] HIPAA does not specifically require a healthcare provider to report successful security incidents. However, if the security incident results in a privacy breach, the healthcare provider will need to mitigate the harm and comply with HIPAA's breach notification requirements.

The HHS Office for Civil Rights ("OCR") has recently published guidance on how healthcare providers can respond to ransomware attacks. The guidance reiterates a healthcare provider's responsibility to implement security incident procedures and indicates that the procedures should "prepare [the healthcare provider] to respond to various types of security incidents, including ransomware attacks."[xvii] The guidance includes certain processes that the healthcare provider should include in its procedures to detect and combat ransomware attacks. The guidance indicates that the healthcare provider should have 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.[xviii]

It is clear that OCR includes a ransomware attack as a security incident. While the healthcare provider may not have a reporting obligation from a security incident that does not trigger a HIPAA breach, its failure to implement policies and procedures to detect and combat security incidents, including ransomware, would indicate that the healthcare provider may not be HIPAA compliant with regard to its policies and procedures.

HIPAA Breach

The second and more onerous issue is whether or not a ransomware attack qualifies as a HIPAA breach. HIPAA requires a healthcare provider like a hospital or medical clinic to provide certain notifications following a breach of unsecured protected health information, unless there is a low probability of compromise of the protected health information. A breach is defined as the "unauthorized acquisition, use, or disclosure of protected health information which compromises the security or privacy of the protected health information."[xix] The OCR guidance on ransomware does not give a clear answer as to whether or not a ransomware attack qualifies as a HIPAA breach and states that "[w]hether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination."

A threshold issue in qualifying a ransomware attack as a breach is determining whether or not the attack involved protected health information. To date, the reported ransomware attacks have dealt with a virus that has infected and halted the use of a medical care provider's computer systems but they have not involved the removal, use or dissemination of protected health information. OCR clarified this issue in its guidance, stating that "[w]hen 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 individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule." As a result, OCR seems to indicate that a ransomware attack that takes control of a healthcare provider's computer system, including ePHI, the attack would be considered a HIPAA breach. However, OCR reiterates that a healthcare provider would need to conduct a risk assessment to see if it can demonstrate that there is a "… low probability that the PHI has been compromised" to determine whether or not the attack triggered the breach notification requirements which would include individual notification, notification to the Secretary of HHS, and possibly to the media for breaches affecting over 500 individuals.

The key question for healthcare providers when determining whether or not a ransomware attack qualifies as a HIPAA breach is the determination as to whether or not the protected health information was compromised.[xx] To qualify as a "breach" that would require notification, the unauthorized acquisition, use, or disclosure must compromise the security or privacy of the protected health information.[xxi] An unauthorized use or disclosure is presumed to be a breach, unless the covered entity demonstrates that there is a low probability that the protected health information has been compromised. Furthermore, the healthcare provider must conduct a risk assessment, focusing on the risk that that protected health information has been compromised. Notification is not required if the covered entity can demonstrate, through its risk assessment, that there is a low probability that the protected health information has been compromised.[xxii] A covered entity may develop its own risk assessment but it must include four specific factors.

First, the covered entity must determine if protected health information was involved.[xxiii] On its face, this seems like a simple analysis but the healthcare provider should investigate the nature and the extent to which protected health information was involved in the event. This analysis would include examining the types of identifiers and the likelihood for re-identification. The healthcare provider should also identify if the information contains sensitive information such as credit card numbers, social security numbers or other information that could be used for identity theft. As noted above, OCR's position is that if the attack encrypts ePHI on a healthcare provider's system, this would qualify as an unauthorized disclosure of protected health information.

Second, the covered entity must determine who used or received the protected health information.[xxiv] The covered entity should analyze the person or entity that improperly viewed or received the protected health information to determine if that entity has an obligation to further guard protected health information. For instance, the improper disclosure might have been made to another HIPAA covered entity who understands the requirements for safeguarding protected health information.

Third, the covered entity should investigate whether or not protected health information was actually acquired.[xxv] Many times, this would include forensic analysis to determine if the file containing the

protected health information was opened or viewed. If the healthcare provider can show through its risk analysis that the file or email containing the protected health information was not actually opened or viewed it could support the healthcare provider's analysis that the incident does not qualify as a breach that would require notification.

Lastly, the healthcare provider should determine to what extent risks have been mitigated.[xxvi] This allows the healthcare provider the opportunity to work to decrease or eliminate further damage after protected health information has been improperly viewed or disclosed. This factor in the risk analysis emphasizes the need for the healthcare provider to quickly identify, investigate and respond to a possible breach. There are a number of ways that a healthcare provider might be able to mitigate risks and it would be fact specific as to the information disclosed and entity that improperly received or viewed the protected health information. With regard to ransomware, the OCR guidance states that the healthcare provider may want to consider the impact of the ransomware on the integrity of the PHI. OCR provides some specific risk mitigation techniques that may be used for a ransomware attack:

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.[xxvii]

Each of these four factors must be evaluated to determine whether or not a reportable breach has occurred. None of the factors are dispositive and additional factors may need to be considered depending on the facts. While HHS has provided these four required factors in conducting a risk assessment, it has not specifically defined what it means for protected health information to be "compromised."

During the risk assessment, a healthcare provider must evaluate the overall probability that the protected health information has been compromised by considering all the factors in combination. A risk assessment must be documented and the conclusions reached must be reasonable. If an evaluation of the factors fails to demonstrate that there is a low probability that the protected health information has been compromised, breach notification is required. The type of notification will be dependent on the number of individuals affected by the breach. The healthcare provider has the burden of proof that notification was not required and must maintain documentation sufficient to meet that burden of proof.

The OCR guidance on ransomware indicates that a ransomware attack, without a risk assessment showing a low probability that that protected health information was compromised, is probably a reportable breach requiring notification. However, the guidance also indicates that if a healthcare provider can demonstrate, through its risk assessment, that there is a low probability of compromise of the protected health information, then the healthcare provider may not need to report the incident. Based on the guidance, it is paramount for the healthcare provider to act quickly to conduct a diligent investigation into the ransomware attack in order to quickly assess whether HIPAA notification is required. Because ransomware attacks are continuing to increase, healthcare providers must be diligent in making sure that they have appropriate policies and procedures currently in place in order to address security incidents of this nature, so that they continue to meet their HIPAA obligation to protect patient information even in these unusual circumstances.

---

[i] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[ii] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[iii] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[iv] http://www.healthcareitnews.com/news/two-more-hospitals-struck-ransomware-california-and-indiana

[v] http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/

[vi] http://wvmetronews.com/2016/03/22/data-safe-after-computer-issues-at-ruby-memorial/

[vii] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[viii] http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom

[ix] http://www.newsweek.com/ransomware-wreaking-havoc-american-and-canadian-hospitals-439714

[x] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[xi] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[xii] Police departments, sheriff's offices, newspapers, schools and churches have all been targeted in ransomware attacks in 2016.

http://www.newsweek.com/ransomware-wreaking-havoc-american-and-canadian-hospitals-439714

http://www.latimes.com/local/lanow/la-me-ln-two-more-so-cal-hospitals-ransomware-20160322-story.html

[xiii] http://www.pri.org/stories/2016-03-06/after-hollywood-presbyterian-hospital-hack-how-much-threat-are-ransom-driven

[xiv] http://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176

[xv] 45 C.F.R. § 164.308(a)(6)

[xvi] 45 C.F.R. § 164.304

[xvii] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

[xviii] Id.

[xix] 45 C.F.R. § 164.402.

[xx] Id.

[xxi] Id.

[xxii] 45 C.F.R. § 164.402(2)

[xxiii] 45 C.F.R. § 164.402(2)(i)

[xxiv] 45 C.F.R. § 164.402(2)(ii)

[xxv] 45 C.F.R. § 164.402(2)(iii)

[xxvi] 45 C.F.R. § 164.402(2)(iv)

[xxvii] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf