PULLMAN &COMLEY

HIPAA in the Age of Ransomware

Connecticut Health Law

07.11.2017
By Russell Anderson and Margaret Bartiromo

According to a recent US Government Interagency report, ransomware is the fastest growing malware threat, targeting users of all types, including health care facilities. This past spring, for example, the WannaCry ransomware crippled the UK's National Health Service and drove hospitals in Connecticut to take action to secure their systems against the virus. And just last month, the NotPetya ransomware shut down some of the IT systems of a health care system in Pennsylvania. In a typical ransomware attack, a hacker demands between $500 to $1,000 in Bitcoin to unencrypt a user's own data, but these demands can go much higher and in some cases ransomware will actually destroy or attempt to exfiltrate data.

Connecticut has taken notice of the onslaught of ransomware. Yesterday, Governor Malloy signed Connecticut Public Act 17-223 into law, which creates a specific class E felony offense for computer extortion involving ransomware punishable by up to three years in prison and a $3,500 fine. Individuals who commit this crime could also be charged with certain other computer crimes and extortion. However, the new law will not address the HIPAA obligations of health care providers when faced with ransomware.

Guidance from the Office for Civil Rights

The Office for Civil Rights (OCR) of the US Department of Health and Human Services has also taken notice of the surge in malware attacks and recently posted a checklist for HIPAA-covered entities and their business associates (BAs) to use when responding to a cyber-related security attack. OCR also offers more in-depth guidance that specifically addresses how covered entities and BAs can prevent and recover from ransomware attacks and evaluate whether breach notification is triggered when ransomware strikes.

An Ounce of Prevention...

The HIPAA Security Rule establishes a national set of standards for protecting health information that is held or transferred in electronic form (ePHI). For example, covered entities and their BAs are already required to have in place:

- A security management process, including risk analysis to identify vulnerabilities to ePHI and security measures to mitigate those risks (45 CFR §164.308(a)(1));
- Procedures to guard against and detect malicious software (45 CFR §164.308(a)(5)(ii)); and

- Controls to limit access to ePHI to only those persons or software programs requiring access (45 CFR §164.308(a)(3)(i)).

According to the OCR guidance, while the Security Rule establishes the minimum standards for protecting ePHI, **it is expected that covered entities and BAs go beyond the strict requirements of the law** and implement **additional risk analysis and risk management processes** to protect themselves against ransomware attacks. For example, the Security Rule does not explicitly require entities to update obsolete firmware (i.e., computer programs and data stored in the hardware), but OCR advises organizations to identify and address the risks of using outdated firmware, especially when updates are available to remediate known vulnerabilities.

Cyber-Attack!

The HIPAA Security Rule requires covered entities and BAs to have reasonable and appropriate procedures in place to respond to a security incident, including a cyber-attack. These procedures must include identifying and responding to the incident, mitigating harmful effects where practicable and documenting the incident and its outcome (45 CFR § 164.308(a)(6)(ii)).

For ransomware in particular, the OCR guidance directs covered entities and BAs to determine: (1) the scope of the incident; (2) the origination of the incident; (3) whether the incident has ended or is ongoing; and (4) how the incident occurred. Following an initial analysis, OCR then advises the affected organization to take the following **additional steps**:

- Contain the impact and propagation of the ransomware;
- Eradicate the malicious software and mitigate or remediate the vulnerabilities that permitted the attack;
- Restore lost data and return to "business as usual;" and
- Conduct a post-incident analysis that incorporates lessons learned to improve incident response effectiveness. The analysis might include an in-depth analysis to determine whether the organization has any regulatory, contractual or other obligations as a result of the incident, including breach notification under HIPAA.

Is it a Reportable Breach?

Determining whether a breach has occurred that triggers HIPAA's breach notification requirements is a fact-specific inquiry; however, when ransomware encrypts an entity's ePHI, a breach has occurred. That breach is **presumed to be reportable** unless the covered entity or BA can demonstrate that there is a low probability that the ePHI has been compromised based on an analysis of four factors, namely: (1) the nature and extent of the ePHI involved, including the types of identifiers and the likelihood of re-identification; (2) the identity of the unauthorized person who used the ePHI or to whom the disclosure was made; (3) whether the ePHI was

actually acquired or viewed; and (4) the extent to which the risk to the ePHI has been mitigated.

As part of this analysis, it will be critically important to decipher, if possible, the particular strain of malware used as part of the attack and its attributes. Does, for example, the malware exfiltrate the data? Has patient data been permanently lost?

The Bottom Line

Health care has become increasingly dependent on information technology, and electronic patient health records contain a wealth of information that is valuable to cyber criminals. In fact, health information may have even more value on the black market than credit card information. Ransomware and other cyber threats are capable of wiping out patient and public health data on a massive scale. Covered entities and BAs must ensure not only that they are in compliance with the Security Rule, but that they also take proactive steps to prevent and recover from a ransomware attack. There is no time like the present to update your software with the latest patches, implement anti-phishing training and software, and review your data recovery processes.

Posted in CT General Statutes, Federal Legislation, Privacy

Tags: Cybersecurity, HIPAA, Office for Civil Rights (OCR), U.S. Department of Health and Human Services (HHS)