SVMIC Sentinel

Ransomware Attacks, Breach Notifications, and Security Rule Compliance: *What You Need to Know Now*

by Loretta Duncan, FACMPE and Brian Johnson, MS, CISSP

The Breach Notification Rule was introduced to healthcare in the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009. Since that time, over 1600 covered entities and business associates have reported breaches affecting 500 or more individuals, with the total number of individuals impacted by these breaches nearing 170 million. The majority of these breaches involve electronic protected health information (ePHI)[1].

Ransomware, as described in the May 2016, issue of The Sentinel, occurs when a cyber-criminal obtains access to a covered entity's ePHI and holds the data hostage until a ransom is paid. This type of attack on healthcare data is considered one of the "biggest current threats to health information privacy," according to Jocelyn Samuels, Director of the Office of Civil Rights (OCR), the agency that enforces HIPAA Rules[2].

A ransomware attack can virtually paralyze a medical practice's operations. Following an attack, there will be a frenzy of activity to limit the damage and restore normal operations; however, there may be even more devastation and hardship from a HIPAA standpoint. Guidance recently released by the OCR states that a ransomware attack will be considered a breach unless it can be proven that the ePHI was not compromised.

The sheer presence of ransomware indicates that a medical practice's systems were compromised, and ePHI could have been at risk. OCR states, "Whether or not the presence of ransomware would be a breach under the HIPAA rule is a fact specific determination." Therefore, it is up to the organization to determine whether or not a breach occurred and to respond appropriately. This requires medical practices to perform a forensic investigation to uncover the underlying details of the attack and to ensure ePHI was not compromised.

The primary purpose of ransomware is to extort the victim for money - at least, that is how it appears on the surface. Ransomware works by encrypting computer files, thus making them unreadable by the computer system that holds the data. To complete the encryption process, the ransomware must access and process the data in question. One must assume that additional payloads (malicious intentions) could be present and executed on the system. For instance, did the perpetrator read, alter, or transfer the data offsite prior to encrypting? Did they leave a backdoor that provides future access? These are just some of the facts that will be uncovered during a forensic investigation.

Organizations need a well-defined incident response plan to guide their actions in the event of an attack. In general, incident response plans include the following phases:

Preparation	• Educating employees • Conducting risk assessments • Development of incident response plans • Implementation of preventative controls
Detection and Analysis	• Identifies indicators of compromise plus preliminary analysis to understand the incident
Containment, Eradication and Recovery	• Educating containment isolates the infected system and prevents propagation to other systems • Eradication removes the ransomware • Recovery restores encrypted data and returns systems to normal operations
Post-Incident Analysis	• Evidence to establish a detailed report of the incident • Fulfills post breach responsibilities • Includes lessons learned for future improvement

It is during the post-incident analysis phase that the forensic investigation will occur and subsequently determine if a breach

1 The U. S. Department of Health and Human Services, Office of Civil Rights, is required by section 13402(e)(4) of the HITECH Act to post a list of breaches of unsecured protected health information affecting 500 or more individuals. This list can be found at this link https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

2 https://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html#

took place. Investigators will be interested in the particular strain of ransomware infecting the system(s). Antivirus vendors and security researchers closely identify, follow, and analyze ransomware as well as other types of malware. Once the strain has been identified, the characteristics and behaviors will be known. This knowledge can be used to demonstrate whether or not the ransomware exhibits behavior that puts ePHI at risk. Known characteristics and key indicators of compromise include:

- infection and propagation methods
- types of targeted data such as banking, health, or personal information
- if data exfiltrated to the Internet
- if backdoors used to give perpetrators unauthorized, future access

Log files produced by technical security controls hold valuable information and aid the forensic investigation. These logs are found on desktops, servers, firewalls, web filters, and intrusion detection systems. However, these devices must first be configured to collect the necessary information. It is important that medical practices talk with their information technology and security providers to ensure the appropriate controls are in place and properly configured. If an entire medical practice's patient database has been compromised in a ransomware attack, the practice will usually be required to provide written notification to all patients, notice to the OCR through their online portal, and notice to local media. This notification must take place within 60 days of discovering the breach. A breach of this magnitude will also require the practice to be listed on the OCR's publicly accessible website that displays all covered entities and business associates with breaches involving 500 or more individuals. More importantly, this type of breach will prompt an investigation by the OCR.

Warning!

Cybercriminals are now using malicious, macro-enabled Word documents to spread malware. Click to learn more

Even though a ransomware attack is not necessarily an intentional breach of ePHI, it can still lead to substantial costs to a medical practice. In her blog entry regarding ransomware, OCR Director Samuels reminds covered entities that proper compliance with the requirements of HIPAA can "help organizations prevent, detect, contain, and respond to threats". When the OCR investigates a breach of ePHI, whether it be due to a ransomware attack or the loss or theft of a device containing patient information, the dollar amount of a settlement or potential civil monetary penalty will be based on the covered entity's level of compliance with the HIPAA Security Rule.

Medical practices should review their compliance with the Security Rule, especially now, since cyber-crime is at an all-time high and healthcare information is so valuable. Director Samuels outlined steps that can be taken to help protect covered entities from a cyber-attack. **All of these steps are requirements of the Security Rule.**

Conduct a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and establish a plan to mitigate or remediate those identified risks
Implement procedures to safeguard against malicious software
Train authorized users on detecting malicious software and report such detections
Limit access to ePHI to only those persons or software programs requiring access
Maintain an overall contingency plan that includes disaster recovery, emergency operations, frequent data backups, and test restorations

Compliance with the Security Rule not only protects medical practices from a potential breach and a large potential settlement with the OCR, it also protects patients. If ePHI is held for ransom, corrupted or lost due to a computer malfunction, patients may not receive the care they need in a timely fashion. It is imperative that medical practices take the time and allocate the financial resources to ensure the security of all ePHI that is created, received, maintained or transmitted.

RESOURCES

Call SVMIC Medical Practice Services Department 800.342.2239
SVMIC Website
HHS Security Rule Guidance
HHS Ransomware Fact Sheet
HealthIT.Gov Mobile Device Privacy & Security
HHS Risk Analysis Guidance
NIST Computer Security Incident Handling Guide
HHS $750,000 Settlement Release
SVMIC Sentinel Ransomware Article (May 2016)