HEALTHCARE PROVIDERS HELD RANSOM BY ALARMING SURGE OF CYBER ATTACKS; What You Can Do to Protect Your Critical Data

IT IS VIRTUALLY IMPOSSIBLE these days to scan a healthcare or technology news report without seeing some mention of the latest hacking or malware attack. Historically, such attacks against healthcare providers generally involved malware designed to attack medical devices with unpatched or outdated software and then infiltrate the entire network, e.g., "medjack" attacks. Hackers increasingly turned their focus to healthcare providers to obtain access to the rich trove of personal data contained in medical records. Such data can often be sold on the black market for upwards of $325 per record.

MORE RECENTLY, however, ransomware has become the preferred tool-of-choice when cyber-criminals attack healthcare providers. Ransomware is a unique type of malware that is distinguished by its defining characteristic of denying access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware. The healthcare data is effectively held ransom until the hacker's demands for payment are satisfied. Unlike data-mining attacks that are designed to remain undetected for long periods, ransomware attacks are intentionally revealed when a user logs-in to his device and receives a message stating something similar to the following:

"If you see this text, then your files are no longer accessible, because they have been encrypted."

This was the message that doctors and nurses at a West Virginia hospital recently discovered when logging-in to their system. The high value and need for timely access to healthcare data makes healthcare providers a prime target for ransomware attacks. Beyond payment of the ransom, the effects of a ransomware attack can be devastating and wide-ranging. Like other victims, the hospital in West Virginia was forced to revert to paper medical records while the hospital began the process of replacing nearly 1,200 hard drives compromised by the attacks and essentially rebuilding its entire network from scratch.

It is more important now than ever for healthcare providers to work closely with their information technology professionals and vendors to ensure that their security and data protection policies are current and effective to protect their medical devices, computer systems, and healthcare data, and are capable of quickly addressing, responding to, and timely resolving any threats.

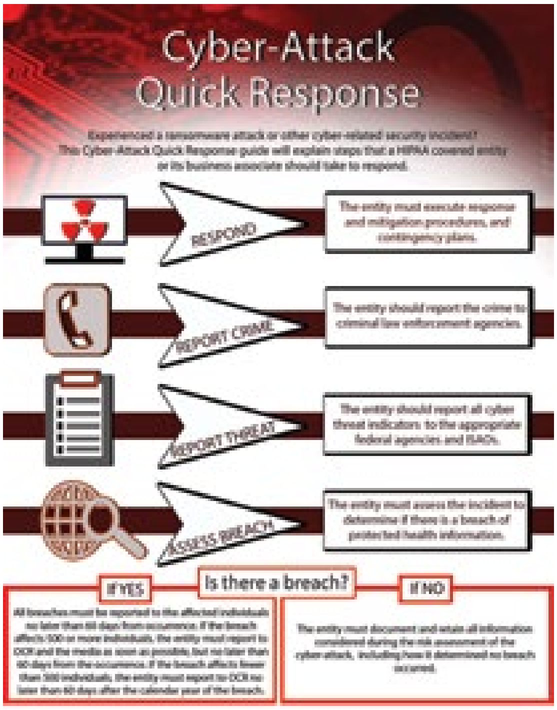
Cyber Attacks on the Rise

According to the U.S. Department of Health and Human Services, there have been 4,000 daily ransomware attacks since early 2016, which is a 300 percent increase over the 1,000 daily ransomware attacks reported in 2015. There were 325 large-scale PHI (Protected Health Information) data breaches, compromising more than 16 million individual patient records. Not surprisingly, these attacks have dramatically increased in 2017. According to *Becker's Hospital Review*, of the 791 data breaches so far in 2017, the health/medical industry has experienced 179 breaches, accounting for 22.6 percent of all U.S. data breaches. Globally, a new and highly-sophisticated strain of ransomware, named "WannaCry," was released in May. So far, it has crippled National Health Service hospitals, the largest hospital group in the United Kingdom, and is reported to have infected computers and medical devices in as many as 99 countries.

In response to these growing threats, a July 2017 survey by *Becker's Hospital Review* reports that more healthcare companies are investing in their security efforts as 83 percent of such companies report that they have implemented stronger policies restricting data access; 76 percent invested in more technology and security; and 41 percent hired more IT people or increased data protection and computer training for their staff.

If there is one thing that IT and computer forensics experts can agree upon, it is the certainty that these cyber-attacks and ransomware infections will continue to grow and spread as new variations of malware are developed and released.

Marc S. Whitfield
Taylor Porter Partner
Privacy and Health Information Technology Attorney



Cyber-Attack Quick Response

Experienced a ransomware attack or other cyber-related security incident? This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.

RESPOND — The entity must execute response and mitigation procedures, and contingency plans.

REPORT CRIME — The entity should report the crime to criminal law enforcement agencies.

REPORT THREAT — The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.

ASSESS BREACH — The entity must assess the incident to determine if there is a breach of protected health information.

Is there a breach?

IF YES — All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.

IF NO — The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.

OCR Responds With New Guidance on Data Breaches

In response to the surge in ransomware attacks, the Office of Civil Rights (OCR) issued new guidance (the Guidance) last year that, among other things, explains how covered entities should guard against ransomware attacks and how to assess whether the ransomware incident is a reportable HIPAA breach. This Guidance should form a core component of any healthcare provider's data security plan.

The Guidance stresses that the HIPAA Security Rule requires covered entities and their business associates to take steps to reduce the likelihood of a ransomware attack, including the need to conduct a risk analysis to identify threats and vulnerabilities to electronic PHI and establishing procedures to guard against malicious software. In addition, all users should be trained to recognize and report any malicious software or suspicious emails. The Guidance also advises frequent backups of data, preferably offline or through separate networks, and periodic testing to ensure the integrity of the backup data and to test the data restoration protocols. It is also important for healthcare providers to understand that the presence of ransomware on its computer system is considered a security incident under the HIPAA Security Rule, and an organizational response to a ransomware attack should follow the organization's security incident response plan, in compliance with HIPAA.

Whether a ransomware attack also constitutes a reportable breach under HIPAA is a fact-specific determination that must be decided on a case-by-case basis. If electronic PHI becomes encrypted as the result of a ransomware attack, a breach has occurred since unauthorized individuals have taken possession and therefore "acquired" protected PHI, thus resulting in an unpermitted "disclosure" 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, in accordance with HIPAA breach notification requirements.

As always, protective data encryption employed by the healthcare provider is an important and beneficial tool. The Guidance clarifies if the PHI encrypted by the ransomware was already encrypted by the healthcare provider to comply with HIPAA such that it is no longer "unsecured PHI," then the healthcare provider would not be required to conduct a risk assessment to determine if there is a low probability of compromise, and breach notification would not be required. However, the Guidance provides examples of fact-specific situations that would require that the healthcare provider investigate further to ensure that its encryption solution, as implemented, correctly renders the affected PHI unreadable, unusable, and indecipherable to unauthorized persons, in all instances.

What Proactive Steps Can You Take?

In addition to maintaining a modern security plan that stresses best-practice security solutions and protocols, employee education and testing remain the key tools to guarding against malware infection. IT personnel should hold educational meetings and circulate reminder e-mails concerning risky e-mail subject lines, social media sites and advertising pop-ups that can infect computers. Phishing schemes that trick employees into opening malware attachments remain a common tactic for malware infections so employee training remains crucial.

In addition to specialized employee training, and specifically regarding ransomware threats and attacks, healthcare providers should:

- Perform frequent backups of system and important data files and verify the integrity of those backups regularly. If ransomware affects your system, you can restore your system to its previous state with any files unaffected by ransomware.
- The safest practice is to store backups on a separate device that cannot be accessed from a network.
- Be careful when clicking directly on links in emails, even if the sender appears to be known; attempt to verify web addresses independently (e.g., contact your organization's IT department or search the Internet

10 Most-Clicked Email Subject Lines for Phishing Attacks:

1. Security Alert – 21%
2. Revised Vacation & Sick Time Policy – 14%
3. UPS Label Delivery 1ZBE312TNY00015011 – 10%
4. BREAKING: United Airlines Passenger Dies from Brain Hemorrhage – VIDEO – 10%
5. A Delivery Attempt was made – 10%
6. All Employees: Update your Healthcare Info – 9%
7. Change of Password Required Immediately – 8%
8. Password Check Required Immediately – 7%
9. Unusual sign-in activity – 6%
10. Urgent Action Required – 6%

Source: KnowBe4, Security Awareness Training and Simulated Phishing Platform, Tampa, Fla.

for the main website of the organization or topic mentioned in the email).

- Exercise caution when opening email attachments. Be particularly wary of compressed or ZIP file attachments.
- Conduct routine risk cybersecurity analysis and penetration testing to regularly test the security of your system.
- Maintain up-to-date patches and security updates and have your IT personnel regularly monitor industry warnings of the latest security and malware threats.
- Test and verify the effectiveness and sustainability of your business continuity plans. Absent an effective and reliable plan, you may find yourself relying solely upon written medical records or being forced to reschedule important medical procedures.

With cyber attacks and ransomware attacks becoming a daily threat for businesses, it is essential that hospitals and other healthcare providers maintain sufficient security measures to reduce the significant risks posed by these threats.

If you require additional information or wish to re-evaluate or strengthen your existing security policies and procedures, do not hesitate to contact me, or any of Taylor Porter's health information technology attorneys. ■

Marc S. Whitfield is a partner at Taylor Porter and works primarily with the Firm's Health Care Practice Group, Commercial Litigation Section and its Intellectual Property Law Group. Marc has practiced since 1988 in the areas of intellectual property law, commercial litigation, contracts and commercial transactions, information technology, health care issues involving electronic health records, HIPAA, data security and privacy rights, and non-compete disputes. You can view Marc's profile at: http://www.taylorporter.com/our-attorneys/marc-s-whitfield