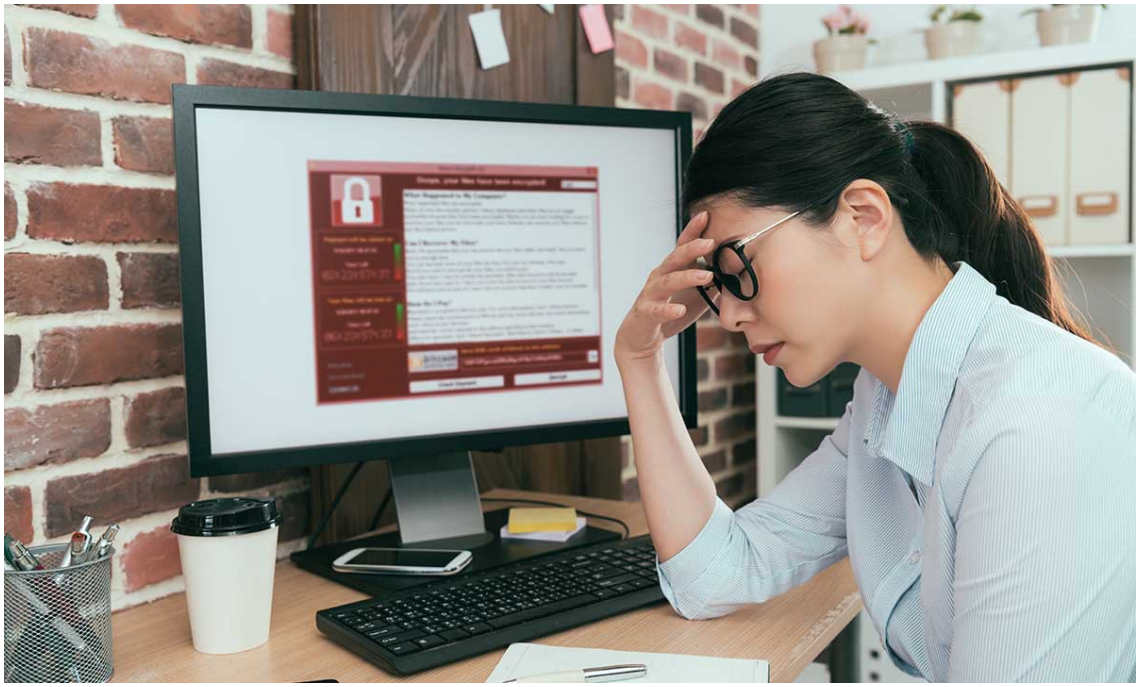
# The Evolving Threat of Ransomware. Cyber attacks have spiked during the pandemic: How prepared is your practice?



**By Justin Joy, JD, CIPP**

Ransomware continues to be a problem with devastating consequences for healthcare practices. While the threat is not new, recent changes in the nature and sources of these attacks have become increasingly concerning. In addition to extorting victims to decrypt data, recent reports of attacks have indicated that bad actors are now demanding payment, or else the hacker will publicly disclose data the attacker has stolen from the victim. Furthermore, ransomware attacks have become increasingly targeted, with hackers using sophisticated intrusion methods increasingly exploiting vendors' systems to reach healthcare groups. On top of all of this, cyber attacks have spiked during the current health crisis. The FBI recently reported a 400% increase in reports of cyber crime.[1] As the

threat of ransomware continues to evolve and with criminals exploiting new opportunities during the pandemic, healthcare organizations must continuously improve their vigilance and evaluate their group's level of cyber readiness.

While the exact scope of the problem is unmeasurable, it is estimated that hundreds, and likely thousands, of healthcare organizations of all sizes—from single-provider physician offices to the largest hospital systems—have been victimized by ransomware attacks. Unfortunately, these attacks continue to impact healthcare groups every day, rendering critical medical information inaccessible.

Compliance with the HIPAA Security Rule not only helps to reduce the likelihood of a ransomware attack in the first place, but when *(not if)* an attack occurs, the Security Rule also provides a framework for better positioning groups to respond and recover from attacks. Medical practices need to implement both administrative and technical safeguards specified under the Security Rule and periodically evaluate the effectiveness their safeguards. (Of course, physical safeguards must be implemented as well to guard against other threats.) With many healthcare groups reconfiguring their IT environment to accommodate remote working during the pandemic, new or expanded risks associated with these recently implemented systems need to be assessed and managed.

On the technical front, HIPAA covered entities need to have effective access controls. Groups should enable multifactor authentication (MFA) where possible for any account that may be externally accessed from the internet. MFA is something to consider when implementing remote access to network or cloud-based resources to facilitate working from home. Keeping anti-malware, software patches, and intrusion prevention systems up-to-date are also important technical safeguards. Mechanisms for recording system activity to create audit reports also should be implemented, which in some cases, is a matter of simply switching on existing capability.

In some ways, administrative safeguards can be more effective than technical safeguards for reducing the risk of ransomware attacks and other cyber threats. Repeatedly, HHS Office for Civil Rights (OCR) investigations find that healthcare organizations have not completed a proper or, in some cases, any, security risk analysis. An analysis of the potential risks and vulnerabilities to all of a group's electronic protected health information (ePHI) is required by the HIPAA Security Rule. Keep in mind that ePHI may be stored in multiple locations, including in cloud-based backups. An analysis of the risks and vulnerabilities to ePHI must be performed any time there is a change in a group's IT environment, such as adding remote access or cloud data storage.

Based on the identification of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of a group's ePHI, a security management plan should be developed and implemented to mitigate those risks and vulnerabilities. Practices also need to be aware of which vendors (business associates) have access to their data, and consideration of the vendor's security measures should be given. Recent attacks have compromised vendor systems, which then provide access to the vendor's customer's (i.e., your practice's) data.

Security awareness efforts and training for all workforce members (including physicians) continues to be one of the most effective ways to avoid cyber attacks. Sadly, cyber criminals are exploiting the pandemic for economic gain. For instance, the Centers for Disease Control and Prevention (CDC) has warned of phishing emails with attachments purportedly sent from the CDC.[2] Instead of the attachments containing information on how to prevent the spread of disease as claimed in the fake email, the attachments install ransomware on the recipient's computer, encrypting files on the victim's computer and potentially files on connected network systems. If workforce members are not made aware—and reminded—of such threats, a medical practice may become more vulnerable to these types of attacks. Additionally, all workforce members should be made aware of the threat of ransomware and the need to immediately report any suspicious system activity or other security incidents to the group's designated security officer. In most instances, a medical practice's employees remain the last line of defense between an attacker and patient data and, in other instances, can be the first to raise an alarm when something is amiss.

Every medical practice needs to have a documented data backup plan, which is periodically tested. In the event of a cyber attack where the practice's data is encrypted, groups typically have two options: pay the extortionist (which, of course, does not guarantee the ability to re-access the encrypted data) or, recover from a good backup. Backup systems and plans need to be tested periodically for their resiliency to ransomware attacks. In many instances, attackers go after backups first, knowing that with the backups deleted or encrypted, their leverage to demand a ransom payment is greatly increased. If a medical practice has recently changed its IT environment, an assessment confirming proper data backup needs to be performed.

Perhaps most concerning for healthcare providers is a recent trend in ransomware attacks where attackers are blackmailing victims into paying ransoms, even if the victim can restore data from a backup, by promising to disclose sensitive data if the ransom is not paid. There have been a number of reports in recent months of these types of attacks, including those where data has actually been disclosed. As the OCR has made clear, a ransomware attack is a presumptive HIPAA breach, requiring notification to media (if information on more than 500 individuals is involved), HHS, and all patients whose information was impacted by the attack. The presumption of a reportable incident, however, may be overcome by showing in a documented risk assessment, that there is no more than a low probability that the availability, confidentiality, or integrity of the

information has been compromised. In an attack involving not only the encryption but also the exfiltration of data, where the attacker, who is not only an unauthorized individual, but also one with malicious intent, maintains possession of that data, it may be difficult to reach a reasonable conclusion that the ePHI has not been compromised.

Unfortunately, cyber crime has increased dramatically during the current health crisis. Like other cyber threats, ransomware is continuously evolving, becoming more sophisticated, difficult to prevent, and yet more detrimental when an attack occurs. Compliance with HIPAA regulations, namely the Security Rule, not only meets a practice's regulatory obligation, but such efforts also help reduce the risk from an attack in the first place. When an attack occurs, practices which have been thoughtful in planning and preparing for such events, are usually in a better position to respond and recover from these devastating incidents. Now more than ever, medical practices need to continue assessing their security measures as well as keeping security awareness top-of-mind for every member of their workforce.

[1]. https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/

[2]. https://www.cdc.gov/media/releases/2019/s0322-phishing.html

---