MARSH & McLENNAN AGENCY

BENEFIT ADVISOR

Volume Twenty, Issue Six August 2017

HIPAA'S SECURITY RULE: RANSOMWARE AND CYBERATTACKS

The Health Insurance Portability and Accountability Act (HIPAA) includes a number of different group health plan rules. Among them are rules requiring employers that sponsor health plans to protect health information in all formats. The final HIPAA Privacy and Security rules were reviewed in our *Benefit Advisor* at http://www.mcgrawwentworth.com/Benefit_Advisor/2014/BA_Issue_2.pdf.

The government continues to be concerned with keeping electronic protected health information (EPHI) secure. Electronic PHI is "individually identifiable health information in an electronic format that is created, received, stored or transmitted by a covered entity and relates to the past, present or future physical or mental health of the individual, or information relating to the provision of care or payment for that care." The *Benefit Advisor* above reviews the specific steps employers need to take to protect EPHI.

In addition, the government recently released the following two guidelines to help employers understand the security risk from ransomware and cyber-attacks:

- Health and Human Services (HHS) Fact Sheet: Ransomware and HIPAA - https://www.hhs.gov/sites/default/files/Ransomware-FactSheet.pdf
- HHS Cyber-Attack Checklist - https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf

Because more and more employers store or maintain protected health information electronically, the government often updates its guidance to ensure EPHI is secure. The newly issued ransomware and cyber-attack guidance will help employers protect EPHI in our changing world. This Advisor reviews the guidance and its suggestions for employers.

Continued on Page 2

We welcome your comments and suggestions regarding this issue of our Benefit Advisor. For more information, please contact your Account Manager or visit our website at www.mma-mi.com.

RANSOMWARE AND HIPAA

Ransomware attacks are becoming a growing problem in the United States. The U.S. government interagency report indicates on average, there have been 4,000 attempted ransomware attacks daily since early 2016. This is a 300 percent increase over the 1,000 attempted daily ransomware attacks reported in 2015.

Ransomware exploits organizational weaknesses to gain access to an organization's infrastructure. It then encrypts all the organization's data so that the organization can no longer access its own systems. Ransomware is distinct from other malware (malicious software) because it denies an organization access to its own data, usually via encryption, until the organization pays a ransom.

A number of Security Rule safeguards and implementation specifications help prevent malware attacks. These measures include:

- A security management process –risk analysis to identify threats to and vulnerabilities of EPHI. It also includes implementing security measures to decrease those risks.
- Procedures to guard against and detect malware.
- Training on how to detect malware.
- Controls to limit EPHI access to only employees that need it to perform their jobs.

The Security Rule risk analysis and risk management requirements should encompass measures to reduce risks and vulnerabilities to EPHI throughout an organization at a reasonable and appropriate level. However, there is no express requirement in the Security Rules to update firmware even though a risk analysis may reveal added risks to EPHI if firmware is obsolete. It is simple to avoid these risks by requiring firmware updates whenever they are available. The Security Rules merely establish a floor or minimum requirements to protect EPHI. Covered entities should adopt more stringent measures in some cases to protect EPHI adequately.

The Security Rules also include standards and specifications that may help covered entities recover from malware infections. Because ransomware attacks, if successful, deny access to data, the Security Rules require organizations to implement a contingency data backup plan. The contingency plan standard includes disaster recovery and emergency operations planning as well as periodic testing of contingency plans and data analysis to ensure critical data is protected.

The data backup might be crucial to resuming operations after a ransomware attack. Organizations should conduct test restorations to verify the integrity of backed up data. Since some types of ransomware can disrupt online backups, organizations may want to consider maintaining back-ups offline and unavailable from their networks.

A ransomware attack may prompt an organization to activate a contingency plan. Hopefully, once it activates the plan, an organization can continue operations while it investigates the attack. The response to a ransomware attack should include processes that:

- Detect and conduct an initial analysis of the ransomware
- Limit the impact or propagation of ransomware
- Eradicate the instances of ransomware or identify vulnerabilities that opened the door for the ransomware attack
- Recover data lost during the attack and return operations to business as usual
- Review the incident to see whether the organization needs to comply with rules such as a HIPAA breach notification

Businesses need to identify ransomware attacks as soon as possible. Clearly, if the organization first becomes aware of an attack when a hacker demands payment, the security protocols were ineffective. Businesses should have security software in place to detect and attempt to halt a ransomware attack. HIPAA requires the health plan workforce to receive appropriate security training. This training should include detecting potential issues and reporting them to a security representative in the IT department. Indicators of a potential ransomware attack include:

- A link clicked on, a file attachment opened or a website visited that may be malicious

Continued on Page 3

- Increased activity in the central processing unit for no apparent reason
- An inability to access certain files (could be an indicator that ransomware has begun to encrypt certain files)
- Suspicious network communications (likely identified by IT staff using intrusion detection or a similar solution)

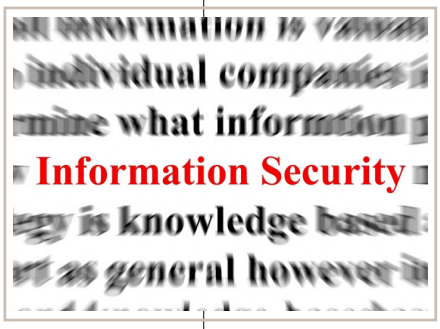
If a ransomware attack is underway, organizations should activate the security incident response plan that the HIPAA Security Rules require. This plan should include measures to isolate various computer systems and halt the attack.

Under the Security Rules, ransomware (or any malware) on a covered entity's computer system is a security incident. A security incident is "an attempt or successful unauthorized access, use, disclosure, modification or destruction of EPHI." Entities must review and investigate all security incidents. If a covered entity is actually infected with ransomware, it should contact the local FBI or United States Secret Service field office. These agencies work with domestic and international partners to assist victims of cybercrime.

HIPAA requires covered entities to investigate security incidents. Covered entities seeking guidance on security incident procedures may want to review NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide. This guide is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

The response should begin with an initial review to determine:

- The scope of the incident – identify affected networks, systems or applications
- The origin of the incident (who/what/where/when)
- Whether the incident is finished, ongoing or propagated any other incidents
- How the incident occurred



These steps will help a covered entity prioritize additional response activities and conduct a more in-depth review of the incident. Once the initial review is complete, the covered entity should:

- Contain the impact and propagation of the ransomware.
- Eradicate the instances of ransomware and remediate vulnerabilities that allowed the attack.
- Restore lost data and return to "business as usual."
- Determine whether there are any regulatory, contractual, or other obligations as a result of the incident. If so, make mitigation efforts and send proper notifications.

Whether a ransomware infection constitutes a breach of EPHI depends on the facts. If EPHI is unencrypted as a result of an attack, a breach has occurred because the hacker has accessed the EPHI and this is not permitted under HIPAA. The entity would have to demonstrate there is low probability that EPHI has been compromised according to the breach notification rules. If the covered entity determines there is a decent probability that the information is compromised, it must make the required notifications.

To demonstrate a low probability that EPHI has been compromised, a covered entity should follow the evaluation recommendations in the breach rules. A risk assessment should consider the following four factors to determine whether EPHI has possibly been compromised:

1. The nature and extent of EPHI involved including types of identifiers and likelihood of re-identification
2. The unauthorized person who used EPHI or to whom the disclosure was made
3. Whether the EPHI was actually acquired or viewed
4. The extent to which the risk to EPHI has been mitigated

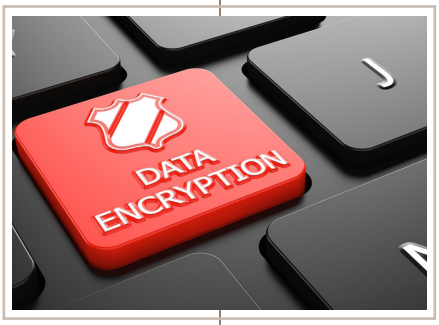
A thorough and accurate analysis of the malware attack is critical. The risk assessment to determine the low probability of compromise must be completed in good faith and reach reasonable conclusions given the circumstances.

Continued on Page 4

Covered entities must maintain supporting evidence to meet the burden of proof including:

- Documentation of risk assessment along with conclusions reached
- Documentation of any exceptions to the impermissible use or disclosure
- Documentation that all notifications were made if the situation was, in fact, a reportable breach

Finally, the rules offer guidance in case of a malware attack on an encrypted device. Whether the EPHI on the encrypted device is considered secure depends on facts and circumstances. If the information is on a powered down encrypted laptop, the EPHI would usually be considered secured and no breach would have occurred. The key point here is that the EPHI is unavailable and inaccessible in this situation. If ransomware is introduced on an encrypted device that is open and accessible, then the EPHI may not be considered secured. If the ransomware gets access to the open computer, it could compromise the EPHI. It depends on the specifics of the potential breach.



Employers are acutely aware of the dangers of operating in a cyber world. Most IT departments are very focused on protecting electronic systems from external threats including ransomware. However, some employers forget their responsibilities related to HIPAA's Security Rule. This ransomware Fact Sheet is a useful reminder that organizations should investigate potential security breaches to determine whether EPHI has been compromised.

CYBER-ATTACK CHECKLIST

The Office of Civil Rights (OCR) recently released a quick response checklist for entities that believe a cyber-related security incident has occurred. The checklist briefly summarizes the steps a HIPAA covered entity or business associate should take.

Key steps include the requirement that employers:

- Follow the employer's response and mitigation procedures and contingency plans – For example, the covered entity should immediately fix any technical problem to stop the incident. The covered entity must also take steps to mitigate any impermissible disclosure of EPHI. This can be done by the entity's IT department or an outside entity. The outside entity would be a business associate of the group health plan if the outside entity will have access to EPHI.
- Should report crime to other law enforcement agencies – For example, state or local law enforcement, the FBI, and/or the Secret Service. Any such reports should not include specific EPHI, unless the HIPAA rules permit it. If a law enforcement official tells the entity that reporting a potential breach will impede a criminal investigation or harm national security, the entity must delay reporting for the length of time law enforcement requests in writing or for 30 days if the request is verbal.
- Should report all cyber threat indicators to federal information-sharing and analysis organizations (ISAOs), such as the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response and private-sector-cyber-threat ISAOs. These reports should not include EPHI. The OCR does not receive these reports from its federal or HHS partners.
- Must report the breach to the OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more people – If the risk assessment determines a breach of EPHI has occurred, the covered entity has a number of potential notification requirements. If the breach affects 500 or more people, the covered entity must notify the OCR, everyone affected and the media. The 60-day time limit can be delayed at the request of law enforcement. If the breach affects fewer than 500 people, each person should be notified within 60 days and the OCR must be notified within 60 days after the end of the calendar year in which the breach occurred.

Employers need to understand how a cyberattack impacts EPHI. This checklist is a reminder of the important steps employers must take. It is critical that employers act quickly to protect confidential data once they identify an attack or a potential attack has occurred.

CONCLUDING THOUGHTS

More and more employers are looking to automate various functions. Security should always be a critical part of any discussion and decision-making process for implementing new technology. It is a good practice to secure all employer/employee data and to comply with laws regarding the security of specific data. Employers also need to be aware of their legal requirements if a breach occurs. The Security Rules require an employer to follow very specific steps if the breach involves EPHI.

Because of the increase in ransomware attacks targeting organizations in the last several years, employers need to make sure they are protecting their electronic data from hackers. Organizations can purchase cyber liability coverage that provides comprehensive assistance in case of a cyber-attack. Often, this coverage will provide support in investigating a security incident. It will also support mitigating potential harm.

If you have any questions, please contact your Marsh & McLennan Agency | Michigan Account Director. MMA

Marsh & McLennan Agency LLC

Health & Benefits
3331 West Big Beaver Road, Suite 200
Troy, MI 48084
Telephone: 248-822-8000 Fax: 248-822-4131
www.mma-mi.com

Property & Casualty
15415 Middlebelt Road
Livonia, MI 48154
Telephone: 734-525-0927 Fax: 734-525-0612
www.mma-mi.com