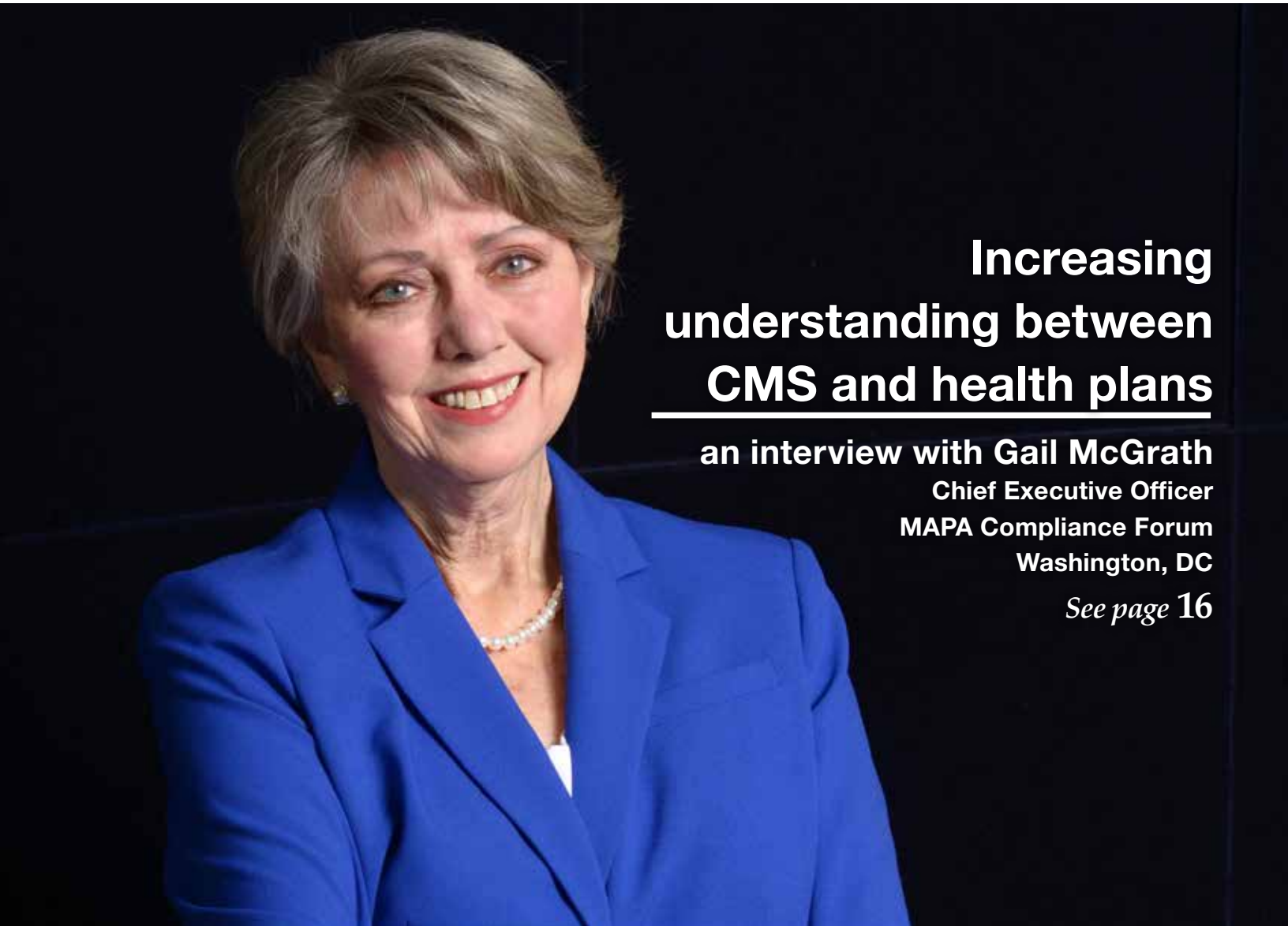
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

March 2017

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



Increasing understanding between CMS and health plans

an interview with Gail McGrath
Chief Executive Officer
MAPA Compliance Forum
Washington, DC

See page 16

by Cathlin E. Sullivan, Esq.

Cybersecurity and ransomware in healthcare: Risks, preparation, and recovery

» Ransomware attacks have sharply increased in the last year alone.

» Ransomware infiltrates a system's network and encrypts the data, then demands a ransom in exchange for the decryption key.

» Organizations should prepare incident-response plans that address these threats and establish teams and systems that can be activated in the event of an issue.

» A ransomware attack is a presumed breach and companies must engage in a risk assessment to determine whether there is low probability of compromise.

» All organizations should train employees to recognize, avoid, and report malware and/or ransomware.

Cathlin E. Sullivan *(cathlin.sullivan@bipc.com) is an attorney with Buchanan Ingersoll & Rooney PC in Philadelphia, PA.*

Ransomware attacks, which have the potential to paralyze an organization's operations, have been increasing at an astonishing level. Beazley, the leading cybersecurity insurance provider, stated in a recent report that it handled more claims for ransomware attacks in July and August of 2016 than it did in the whole of 2015 (52 attacks in July and August 2016, compared to 43 attacks in all of 2015).[1]

Sullivan

Similarly, interagency guidance issued by the United States government noted that there were 4,000 ransomware attacks per day in 2016, up from 1,000 attacks per day in 2015.[2] The healthcare industry is a frequent target of ransomware attacks, with one report stating that 88% of all ransomware attacks are on hospitals.[3]

Recent ransomware attacks on hospitals have garnered significant media attention. By way of example, in February 2016, Hollywood Presbyterian Medical Center experienced a ransomware attack.[4] In that attack, the ransomware encrypted part of the Medical Center's electronic health record (EHR), rendering it unusable for more than a week. The hacker demanded 9,000 Bitcoins (a type of virtual currency) for the decryption key, and the Medical Center ultimately paid 40 Bitcoins (about $17,000 at the time; as of January 21, 2017, 40 Bitcoins were equivalent to about $37,000). One month later, Methodist Hospital in Kentucky experienced a ransomware attack. It was able to mitigate damage by taking its main network offline, and avoided paying a ransom by restoring its data from backup servers.[5, 6]

In May 2016, Kansas Heart Hospital was hit with ransomware, and paid a ransom.[7] However, the hackers didn't return access to the hospital's files, and instead demanded an additional ransom—which the hospital did not pay. The hospital stated that it had a plan for this sort of event, and that plan was implemented and helped to minimize the extent of the damage from the ransomware. In all three instances, the organizations stated that there was no evidence that patient records were compromised.

What is ransomware?

Ransomware is malicious software (i.e., malware) that infiltrates an organization's electronic information system, usually by way of hacking or when an employee clicks on a malicious email attachment or link. Once in the system, the ransomware runs in the background, encrypting the organization's data and rendering the data unreadable and unusable by the organization unless and until it is decrypted. Once the encryption is complete, the hacker notifies the organization that its data has been encrypted and demands that the organization pay a ransom (generally in the form of Bitcoin) in order to receive the key to decrypt the data. Unfortunately, however, paying the ransom is not a guarantee that the key will be provided, nor does it guarantee that the data will not be exfiltrated/disclosed or destroyed. For hospitals and healthcare organizations, the encrypted data includes the patient data on the EHR—which obstructs (or completely prohibits) the organization's ability to access the information stored in its EHR, requires activation of the organization's security-incident response plan, and presents the problem of whether the ransomware constitutes a breach of protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).

Broadly speaking, the HIPAA Privacy Rule defines PHI as individually identifiable information that relates to the provision of healthcare services to an individual. Information stored in an EHR is a primary example of individually identifiable PHI. The Privacy Rule further defines when that information can be disclosed by a covered entity without a patient's consent. The HIPAA Security Rule sets out how a covered entity must protect the confidentiality, integrity, and availability of electronic protected health information (ePHI), and requires administrative, physical, and technical safeguards for that information. These safeguards are further divided into standards and implementation specifications, which provide covered entities with "required" and "addressable" standards. The required standards must be implemented. The addressable standards provide flexibility based on the organization's needs and allow an entity to implement that standard, implement a reasonable and appropriate alternate standard that achieves the same purpose, or not implement the standard. The decisions regarding the addressable standards must be documented in writing.

Can organizations prevent ransomware?

Not necessarily. However, organizations can—and in fact are required to—implement security measures that can help prevent malware from being introduced into their systems. Many of these security measures would also help the organization prevent the access or infiltration of ransomware.

For example, security awareness and training is one of the administrative safeguard set forth in the Security Rule. This is an addressable standard, and can include both processes such as anti-virus or anti-malware software and email scanning to detect and guard

against malware. It also includes workforce training regarding how to detect and report malicious software, such as phishing attempts. These safeguards will help prevent or detect malware or ransomware that seeks to infiltrate a system. Organizations should also implement access controls that limit the amount of information an individual authorized user can access, based on that individual's legitimate business need to have access to that information. This will minimize the number of users who have broad access to the protected data, thus reducing the number of entry points for ransomware.

In addition, the Security Rule requires organizations to complete a risk analysis to identify the risks and vulnerabilities to the confidentiality, integrity, and availability of all PHI that the organization creates, receives, maintains, or transmits. The organizations must then use the findings from the risk analysis to create a risk management plan that addresses and implements measures to reduce the identified threats and vulnerabilities to a reasonable and appropriate level. The risk analysis and risk management plan are both required standards as administrative safeguards. The specific security measures are not dictated by the Security Rule, but should be reasonable, taking into account: (1) the size, complexity, and capabilities of the organization; (2) the technical infrastructure and capabilities; (3) costs; and (4) the probability and criticality of the identified risks.[8]

Is ransomware a breach?

The Office for Civil Rights (OCR) addressed the question of whether malware is considered a breach in guidance issued in July 2016.[9] In that guidance, OCR reviewed the HIPAA definition of a breach, which states that a breach is "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of PHI."[10] The encryption of data through ransomware is considered the "acquisition" of data, because the individuals or organizations that encrypted the data did not have the authority to take possession or control of that data. As such, a ransomware attack is considered to be a presumed breach.

Unless the organization can demonstrate through a risk assessment that there was a low probability of compromise of the data, an organization that experiences a ransomware attack must comply with applicable breach notification provisions, including notice to individuals, the Secretary of Health and Human Services, and the media, if required. Therefore, an affected organization should launch a breach assessment contemporaneous with its security-incident response plan. In addition to their HIPAA obligations, affected organizations should also take into account relevant state data security and notification laws.

Demonstrating low probability of compromise

A risk assessment to assess whether there was a low probability that the affected information was compromised must consider at least the following four factors:

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

This risk assessment process allows organizations to thoroughly evaluate the risk of compromise to the PHI. For instance, OCR noted, if an affected organization determines that the risk of unavailability of the data or compromise of the data integrity was high,

those factors support conclusions that the PHI was compromised. However, if the PHI was encrypted, and the encryption method worked as implemented to render the PHI unreadable, unusable, and indecipherable to unauthorized users and, as such, it is no longer considered "unsecured PHI" under the breach notification provisions, then no risk assessment is needed and breach notification is not required. In the ransomware context, if a computer is only encrypted while no authenticated user is logged on and the machine is powered down, that encryption may be sufficient, depending on the specific factual circumstances, as in the case of a lost laptop. However, in the ransomware context, if a user who is actively using the system (and as such the encryption is not active) clicks on a malware link or opens an attachment that infects the computer with ransomware, the encryption would not be sufficient to render the PHI unreadable, unusable, and indecipherable to the unauthorized user, and the four-factor risk assessment above would be required.

The risk assessment must be thorough, completed in good faith, and reach reasonable conclusions given the circumstances. In addition, organizations must maintain supporting documentation that is sufficient to meet their burden of proof regarding the conclusions reached during the risk assessment and the breach notification process.

How should organizations prepare for and respond to ransomware?

A ransomware attack is considered a security incident under the HIPAA Security Rule, because it is, at the very least, the attempted unauthorized access to or interference with system operations.[11] Therefore, once ransomware is detected, an organization must activate its security-incident response plan.

It's essential that all organizations, regardless of size, have security-incident response plans in place, so that if or when ransomware (or any malware) becomes an issue, they are prepared to respond quickly and comprehensively. The response plan should not only address the required contingency plan items found in 45 C.F.R. 308(7)(ii), such as data backup, disaster recovery, and emergency-mode operations, but it should also define the team that will respond to the incident and set out the roles that each person will have in the response. Outside consultants, such as legal advisors or forensic analysts, should be brought in as needed based on the nature and scope of the incident. In the event of ransomware, law enforcement should be immediately notified of the incident. In fact, the Interagency Technical Guidance document referenced in Endnote 2 states that agencies "strongly encourage [organizations] to contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance." "Tabletop" or mock breach exercises are helpful in determining whether a response plan and team is sufficient and prepared for a security incident.

The initial analysis of a security incident should explore, at least, the scope of the incident, the origination, and how the incident occurred. The organization should also evaluate whether the incident is ongoing and can potentially be stopped (e.g., an employee immediately reports malware that is now in the process of encrypting the files, IT notices an unusual pattern of activity) or if it is complete (i.e., the encryption is finished and the ransom has been demanded). The response team should also look to contain the impact and propagation of the incident.

The organization should also have in place systems that will allow it to recover as quickly as possible from a ransomware—or any malware—attack. These include frequent backing

up of data, including offline backups that are inaccessible to network infiltration, and ensuring the availability and accessibility of that data in the event ransomware prevents the organization from having access to its primary data. As with the tabletop breach exercises, test restorations of the backup data can help ensure that the organization will have the capability to respond quickly when needed.

Following any security incident, the organization should review its regulatory and contractual obligations, engage the media as needed to manage or mitigate any reputational harm, and review and address the vulnerabilities that led to the incident occurring.

Conclusion

Ransomware and malware are increasingly targeting and affecting healthcare organizations. Their impact can be devastating to an organization's operations and can lead to costly and burdensome recovery measures. Although organizations cannot necessarily prevent ransomware, they can position themselves to be able to identify, manage, and mitigate the impact of ransomware. All organizations should implement policies and procedures regarding cybersecurity and conduct robust training programs so that all employees are able to identify the risks and respond quickly when issues arise.

1. Beazley Breach Insights: "Ransomware attacks set to quadruple in 2016" October 2016. Available at http://bit.ly/2j4Z4Nl
2. U.S. Government interagency release: "How to Protect Your Networks from Ransomware" Available at http://bit.ly/2kj83HL
3. Max Green: "Hospitals are hit with 88% of all ransomware attacks" *Becker's Health IT & CIO Review*, July 27, 2016. Available at http://bit.ly/2jZJbXD
4. Richard Winton: "Hollywood hospital pays $17,000 in Bitcoin to hackers; FBI investigating" *Los Angeles Times*, February 18, 2016. Available at http://lat.ms/2jZNJ00
5. "FBI investigating cyber-attack at Methodist Hospital in Henderson," NBC 14news.com, March 28, 2016. Available at http://bit.ly/2jxg7nv
6. "Methodist Hospital Up and Running After Cyber Attack," NBC 14news.com, March 31, 2016. Available at http://bit.ly/2jeKgH5
7. "Hackers demand ransom payment from Kansas Heart Hospital for files," KWCH.com, May 20, 2016, Available at, http://bit.ly/2k3DTel
8. See, e.g., 45 CFR § 164.306
9. FACT SHEET: Ransomware and HIPAA. Available at http://bit.ly/2k3tMpI
10. 42 CFR § 164.402
11. See, e.g., the Security Rule definition, supra, and 45 C.F.R. § 164.304