HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

December 2017

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

How HCCA's CI Silent Auction supports recipients of America's Fund

an interview with Justin Lansford

U.S. Army Veteran
America's Fund Recipient,
and Gabe's pal

See page 16

This article, published in *Compliance Today*, appears here with permission from the Health Care Compliance Association. Call HCCA at 888-580-8373 with reprint requests.

Contents

December 2017

FEATURES

COLUMNS

DEPARTMENTS

by Theresamarie Mantese, Esq., Jordan Segal, Esq., and Paul Mantese

How to respond when ransomware catches you off guard

» Health organizations are currently facing many cybersecurity threats.
» Complying with HIPAA regulations can help overcome these challenges.
» Each hospital must assess its individual risk and plan accordingly.
» Cloud technology, software, and further encryption can help fight ransomware.
» If attacked, hospitals should attempt to isolate the virus and report the attack to HHS.

Theresamarie Mantese *(tmantese@manteselaw.com) is a Partner,* ***Jordan B. Segal*** *(jsegal@manteselaw.com) is an Associate Attorney, and* ***Paul Mantese*** *(pmantese@manteselaw.com) is a Law Clerk at the Mantese Honigman, PC law firm in Troy, MI.*

It's a sunny morning, and you are going about your typical daily business. Suddenly, your computer freezes, and an ominous demand appears on your system: Pay thousands of dollars in Bitcoins to some unseen hacker or else you will never be able to access any of your patient files again. Hundreds—perhaps thousands—of records are being held hostage by the WannaCry computer virus. If you refuse to comply, these records will be permanently erased. On the other hand, you could lose hundreds of thousands of dollars and there's no guarantee that the hackers will restore your files, even if you do pay the ransom!

This is exactly the difficult situation that health officials from the UK National Health Services faced on May 12, 2017. Along with hundreds of thousands of computers that were infected in more than 150 countries during this single attack, millions of records across the world were held hostage.[1] It should be obvious that ransomware attacks, both in the United States and internationally, have intensified. For example, in 2016, Hollywood Presbyterian Medical Center in Los Angeles similarly had its records held hostage until it paid a ransom.[2]

Ransomware attacks may be the newest threat to data security, and the cyber-criminals perpetrating these attacks are specifically targeting healthcare providers. Luckily, The Health Insurance Portability and Accountability Act of 1996 (HIPAA) already provides a framework to protect data from these new attacks. Compliance with HIPAA's existing security rules and protocols will provide some protection against ransomware attacks. In other words: Compliance with HIPAA's Security Rule may well insulate healthcare providers from ransomware viruses.


Mantese


Segal


Mantese

How to comply with the Security Rule

HIPAA and its 2009 amendments in the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, create national standards for protecting patient health information from unwanted disclosure by businesses. While the Privacy Rule governs permissible disclosures, the Security Rule requires HIPAA covered entities (and their business associates) to protect electronic health information from unauthorized access.[3]

Most compliance officers are familiar with the very specific requirements of the Privacy Rule. However, hospitals pay less attention to the Security Rule. In contrast to the specific requirements of the Privacy Rule, the Security Rule is more flexible and permits each HIPAA covered entity to design and implement a security protocol that suits its individual needs. HIPAA should be reviewed in order to help compliance officers train a hospital's workforce to identify the presence of ransomware on a computer system.[4] Additionally, compliance officers should consider the following:

- Determine whether your organization is vulnerable to an attack.
- Make use of the Department of Health and Human Services' (HHS) Risk Assessment Tool,[5] as well as the HIPAA Security Rule Tool Kit.[6]
- Utilize the Risk Analysis Guide from the same website.
- Examine Security Rule guidance material.

Testing backed-up data, as required by HIPAA, can allow your hospital to understand the resiliency of its systems and whether its contingency plan is sufficient to allow for recovery from an attack.[7]

With these considerations in mind, the covered entity or business associate's security practices should address:

- **Administrative safeguards:** Require the covered entity and its business associates to implement policies and procedures to prevent, detect, contain, and correct security violations on a regular basis.
- **Physical safeguards:** Require policies which limit physical access to electronic information systems and facilities.
- **Technical safeguards:** Require technical or technological protections for electronically protected information, such as strong user passwords, automatic log-offs, and proper encryption protocols.
- **Organizational requirements:** Require that vendors and business associates utilize similar data security protocols and standards.
- **Policies and procedures documentation:** Require that appropriate policies and procedures are in place to ensure that the covered entity implements its administrative, physical, technical, and organizational safeguards.[8]

The flexibility of the Security Rule is a double-edged sword. On the one hand, it means that compliance officers and covered entities must develop their own security protocols; there is no "one-size-fits-all" approach that will ensure every covered entity will be protected. No two covered entities will face the same security challenges. On the other hand, if there were a one-size-fits-all approach, any hacker who finds a security flaw would be given the virtual keys to the kingdom.

Best practices

Despite the Security Rule's requirement that each covered entity develop its own program, there are some best practices that can help to protect any system from ransomware (or

other cybercrime) attack. Perpetrators of ransomware attacks rely heavily on the fact that most organizations are ill-prepared for attacks. Proper planning by hospitals should go beyond standard HIPAA procedures, to keep pace with modern technological threats. Proactive procedures can render ransomware ineffective when it is transmitted to its target. A forward-thinking approach can show an impressive sense of preparedness, and a high-tech defense system can make a hospital a top choice for patients who are concerned about their personal data. Thus, the following steps should be included in any Security Rule compliance program:

- **Back up data regularly:** Consider automatic backup and recovery programs to ensure that all backed up data is up to date and quarantined from hacking attempts or other viruses.
- **Adopt the cloud**: Although the cost of cloud computing and backup storage has increased in recent years, compromised patient data can destroy patient trust, costing the facility millions of dollars in future revenue, as well as costs associated with addressing the attack itself.
- **Protect your email system:** Prevent phishing attacks by using spam filters that prevent tainted materials from reaching hospital personnel in the first place.
- **Install a firewall**: Implementing both hardware and software firewalls can be key to blocking viruses from reaching your systems.
- **Limit devices:** Restrict employees or other officials from using their own personal software or hardware, even a thumb drive can carry a powerful virus.
- **Encrypt data:** Develop powerful, specialized encryption codes using multiple algorithms or ciphers.
- **Buy cyber insurance:** Consider purchasing a cyber insurance policy. Many traditional insurance policies do not cover costs associated with a ransomware attack.[9]

In addition, compliance officers should regularly train their workforce to identify the presence of ransomware on a computer system. An employee might observe heightened disk activity for no apparent reason, as well as the presence of re-located files that appear under a new name. This signifies that an attack is already underway. Just as the Transportation Security Administration (TSA) and other law enforcement regularly advise travelers to report suspicious packages in an airport, a vigilant workforce can spot and avoid a ransomware attack before it takes place.

Finally, develop a plan in case of attack and create procedures to isolate potentially infected systems and automatically restore uninfected data. This will include testing backed-up data, which can allow your hospital to understand the resiliency of its systems and whether a contingency plan is sufficient to allow for recovery from an attack. Proper advanced planning can cut response time in the event of an attack and makes it more likely that data held hostage can be rescued before any ransom is paid.

In the event of a ransomware attack

If an attack does occur, respond with urgency and attempt to isolate the infected computer. If the virus can be contained to one device, it may be easier to repair. If the virus stems from an email chain, notify all employees and office personnel, and instruct them not to open harmful email links. Shutting off internal computers and taking them offline may reduce the spread of the virus as well.

In any event, paying the ransom is a mistake. Since 2005, more than 7,000 cases of ransomware attacks have resulted in over $57,000,000 in damages to victims. Fees to

recover files can be as steep as $10,000 per file, and most ransomware cyber criminals live overseas in countries such as Russia or China, where they can evade American authorities.[10] These significant figures may encourage a cyber criminal to decide to increase the ransom, depending on the importance of the hostage documents. Worse still, paying the ransom incentivizes hackers to attack again later or attack others.

There is considerable scholarly disagreement about whether a ransomware attack is a reportable event under HIPAA's Breach Notification Rule. Under that rule, a breach is defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."[11] Such breaches must be reported to HHS. Some scholars have argued that, because a ransomware attack only involves the encryption of patient records, and not the "acquisition, access, use or disclosure," a ransomware attack need not be reported. On the other hand, it has been argued that the ransomware must "access" patient data to recognize patient data. Under this view, a ransomware attack would need to be reported to HHS under the Breach Notification Rule.

HHS, itself, has provided guidance on the issue, stating that it does consider ransomware attacks to be breaches that must be reported, subject to certain exceptions.[12] It remains an open legal question as to whether HHS's view will be upheld in a legal challenge. Until further guidance is provided, the safest approach is to consider a ransomware attack to be covered by the Breach Notification Rule. First, there is no penalty for over reporting, but failing to report a breach carries significant fines and potential penalties. Second, a healthcare provider that reports a ransomware attack is the *victim*, whereas a healthcare provider that does not report may be viewed as attempting to cover up a breach. Finally, more accurate reporting gives law enforcement a better understanding of these attacks, and thus they are better able to find or counteract the global problem of ransomware attacks.

Conclusion

With the increasing number of cyberattacks occurring in the United States, planning and coordination are paramount in properly fortifying hospitals against ransomware and other types of electronic attacks. After all, most healthcare providers, even small ones, maintain a king's ransom of patient information. This immediately places virtually all healthcare providers in the crosshairs of cyber criminals who are out to extort vulnerable societal organizations for payment. Many cost-effective solutions are available to companies that wish to secure their patient data and simultaneously comply with HIPAA regulations. By considering the steps listed above, companies can implement training programs and make technological investments that are key to keeping hospitals running efficiently in our increasingly data-centric world. Security will continue to become more important as hackers become more sophisticated and data grows in value.

1. Nicole Perlroth and David E. Sangermay: "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool" *New York Times*, May 12, 2017. Available at http://nyti.ms/2zGry3D.
2. Danny Yadron: "Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers" February 16, 2016. Available at http://bit.ly/2gEnp8M.
3. 45 CFR Part 160 and Subparts A and E of Part 164 (Privacy Rule); 45 CFR Part 160 and Subparts A and C of Part 164 (Security Rule).
4. Health & Human Services: Fact Sheet: Ransomware and HIPAA. Available at http://bit.ly/2saASO2.
5. HHS Risk Assessment Tool. Available at http://bit.ly/2zaFiY8
6. HIPAA Security Rule Tool Kit. Available at http://bit.ly/2gGuO7X
7. Id.
8. 45 CFR 164.308 (Administrative safeguards)
9. Department of Justice: How to Protect Your Network from Ransomware, an interagency technical guidance document. Available at http://bit.ly/2kj83HL
10. DOJ: Peter J. Kadzik letter: DOJ Responds to Carper Inquiries on Response to Threat of Ransomware, March 4, 2016. Available at http://bit.ly/2z9fgog
11. 45 CFR 164.402(i) (Definitions)
12. Ibid, Ref #4