Innovations in CLINICAL NEUROSCIENCE

A peer-reviewed journal providing evidence-based information

VOL. 13, NO. 11-12

NOVEMBER–DECEMBER 2016

The Right to Die in Chronic Disorders of Consciousness: Can We Avoid the Slippery Slope Argument?

ALSO INSIDE

Case Report
Acute Hyperglycemia Associated with Psychotic Symptoms in a Patient with Type 1 Diabetes Mellitus: A Case Report

Case Report
Complete Recovery from Cardiac Arrest Caused by Risperidone-induced Hypothermia

Case Report
Sympathetic Nerve Entrapment Point Injection as an Antireflux Procedure for Refractory Laryngopharyngeal Reflux: A First Case Report of Innovative Autonomic Regulation

Risk Management
Ransomware: Minimizing the Risks

Differential Diagnoses
Encephalopathy or Psychosis?
QUESTION

I work in a small private practice with very limited IT support. Given recent national news headlines in which cyber attackers have targeted large healthcare systems and held patient information for ransom, should I be concerned as a solo practitioner?

ANSWER

Yes, healthcare providers of all sizes should be concerned about ransomware and other cyber attacks.

What is Ransomware?

Ransomware is a type of malicious software that seeks to infiltrate computer systems or connected devices in order to encrypt a user’s files. Once the files have been encrypted, making the information indecipherable and inaccessible, the user receives a pop-up notification demanding payment of a ransom (usually in untraceable digital currency such as Bitcoin) in exchange for the decryption key.¹

Ransomware in the News

A few of the most notable healthcare ransomware attacks of 2016 include the following:

- Hollywood Presbyterian Medical Center (HPMC), in Los Angeles, California, made national news headlines last February when it was widely reported they paid hackers $3.4 million in Bitcoin for a decryption key after being locked out of their computer systems. HPMC later released a
RISK MANAGEMENT

statement denying those reports, but confirming they did pay a $17,000 ransom in the interest of quickly restoring hospital operations in order to provide patient care. Many people have been critical of HPMC’s decision to pay the ransom and argue that this decision may have been directly responsible for a number of subsequent healthcare ransomware attacks.4

- Methodist Hospital (Henderson, Kentucky) announced an internal state of emergency last March after being infected by a ransomware variant known as “Locky.” The attack limited Methodist’s access to all web-based and electronic communications, and the hospital was forced to power down desktop computers in order to isolate the virus. Hackers demanded a $1,600 ransom but reportedly relented after Methodist restored its IT systems using backup data.4

- Also in March of 2016, Medstar Health (Baltimore, Maryland) became the target of a ransomware attack that prevented Medstar facilities from accessing patient data, making it necessary to postpone patient appointments and surgical procedures in some cases. Hackers threatened to destroy the decryption key and render records permanently inaccessible if Medstar did not pay $19,000 in Bitcoin within the next 10 days. Medstar was also given the option to decrypt a single computer for $1,250 in Bitcoin.5

- Kansas Heart Hospital in Wichita could no longer access patient files after its servers suffered a ransomware attack last May. When Kansas Heart paid the initial ransom requested by cyber attackers, hackers responded by decrypting only a portion of the stolen information. The hackers then made a new ransom demand for the rest of the encrypted patient information. Kansas Heart did not make a second ransom payment.6

Why Should You Be Concerned?

Standard of care. Ransomware attacks may make it difficult for you to provide quality patient care. A ransomware attack may affect your ability prevent you from accessing electronic health records (EHRs), patient emails, and electronic billing and scheduling systems, which are essential to daily practice and your ability to meet the standard of care.

Federal law. Physicians who maintain patient information could be subject to federal privacy laws. Under HIPAA’s Security Rule, covered entities are required to implement security measures that may help prevent the introduction of ransomware. Covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) when faced with a breach must then comply with the breach notification rule as well as face the possibility of civil monetary penalties. The Federal Trade Commission (FTC) has also recently expressed a willingness to bring enforcement action against those businesses that fail to reasonably safeguard consumer information in accordance with their privacy and security practices.7

State law. State law may even govern the privacy and security of patient information. If a breach of patient information violates state law, an attorney general’s office may be compelled to open an investigation. Parties affected by the breach could also have a private cause of action under state law.

What Steps Should You Take to Prevent Ransomware?

Resources from the United States Office for Civil Rights (OCR), Federal Bureau of Investigation (FBI), and Federal Trade Commission suggest the following prevention steps:

1. Understand ransomware attacks happen all the time. The United States Department of Justice now estimates that an average of 4,000 ransomware attacks occur daily. This figure represents a 300-percent increase in ransomware activity seen at this point last year.7 Recent reports also indicate the healthcare industry may be targeted by ransomware attacks more frequently than any other industry. Cyber security provider Solutionary found the healthcare industry accounted for 88 percent of all ransomware detected last quarter.7 Factors such as the value of healthcare records (partial records can sell for up to 50 times the value of credit card information on the black market, according to the FBI), the healthcare industry’s transition to EHRs, and the lack of security technology utilized by smaller practices have contributed to an upsurge in healthcare ransomware attacks.8

2. Ensure all employees receive ransomware training. It is important that employees are made aware of the threat that ransomware poses and that they receive up-to-date training on the following:

- Detecting malware
  - Staff should be able to recognize when a link is
**RISK MANAGEMENT**

39

One of the most effective ways to protect your practice in the event of a ransomware attack is to back up sensitive and important information. Taking this step will allow you to restore your data and recover from a ransomware attack quickly. As some ransomware variants have been known to remove or otherwise encrypt online backups, practices should consider maintaining backups offline and unavailable from their networks.9

4. Encrypt sensitive practice data. Providers should consider encrypting and password protecting all patient information and devices. Per OCR's Ransomware and HIPAA Fact Sheet, a breach of protected health information that is actively encrypted and indecipherable at the time of a ransomware attack cannot be breached. Such a breach does not require a physician to give notice of the breach.9

5. Ensure basic technical safeguards have been implemented. Providers should ensure the implementation of the following technical safeguards:
   - Up-to-date antivirus software on computers
   - Enabled automated patches for operating systems and web browsers
   - Complex passwords
   - Pop-up blockers.10

6. Don’t think it can’t happen to your small practice. While ransomware attacks on large hospitals and health systems have been highly publicized, one must not forget that smaller private practices can also be at risk. In 2012, ABC reported that hackers encrypted emails and electronic health records maintained by Surgeons of Lake County, a small medical practice in Illinois. Hackers offered to make a decryption key available upon receipt of a ransom payment, but the medical practice responded by refusing to pay the ransom, shutting down their servers, and contacting the local authorities.11

As ransomware becomes more widely used by cyber criminals, private practitioners should expect to be targeted more often. The growing number of ransomware attacks is a direct result of the ease with which ransomware programs can now be acquired. Cyber gangs now host websites from which fairly simple ransomware programs can be downloaded by aspiring cyber attackers who, in return, pay a percentage of any ransom collected to the program creators.9

Widespread availability of ransomware doesn’t bode well for private practitioners with inadequate IT support and/or insufficient data security protocols in place, as this may make them attractive targets for cyber attacks.

7. Stay informed and current. Providers should stay up to date on the latest ransomware news and information. The United States government continues to provide resources to help providers protect against the threat of ransomware. Providers may also want to consider signing up for the OCR Security Listserv in order to receive ransomware updates and guidance.12

**REFERENCES**


AUTHOR AFFILIATION: Mr. Pope is Associate Risk Manager at PRMS, Inc. in Arlington, Virginia.

ADDRESS FOR CORRESPONDENCE: Donna Vanderpool, MBA, JD, Vice President, Professional Risk Management Services, Inc., 1401 Wilson Blvd., Suite 700, Arlington, VA 22209; E-mail: vanderpool@prms.com