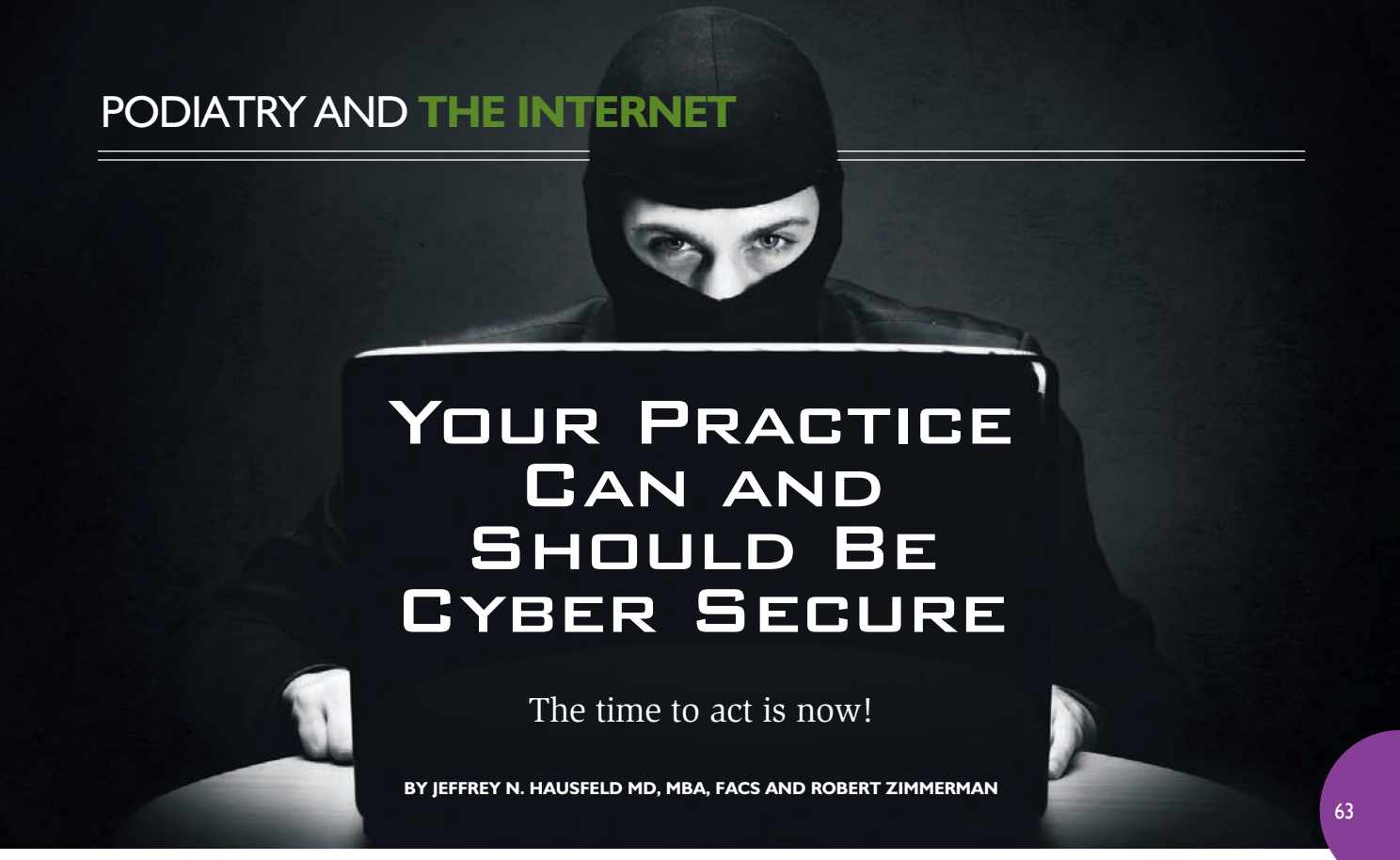

# Your Practice Can and Should Be Cyber Secure

## The time to act is now!

BY JEFFREY N. HAUSFELD MD, MBA, FACS AND ROBERT ZIMMERMAN



*Reprinted with Permission from The Journal of Medical Practice Management, May/Jun 2018, pgs 389-391, copyright 2018 Greenbranch Publishing, LLC, (800) 933-3711, www.greenbranch.com.*

Chances are if you did your residency training in the 1980s and 1990s, the notion of implementing cybersecurity protocols and patches in your office is something quite foreign to you. Do you know of any colleagues that have been hacked in their offices or "held up" by ransomware? The time for taking steps to secure your organization and protected health information is now. Allow me to share a story of a recent "hacking" event.

A busy surgical specialty private practice in the Washington, DC, area is managed by a seasoned administrator who has over a decade of experience and stellar performance. One morning she clicked on a link from an email that appeared to be an invoice from a known business partner. She inspected the invoice and was planning to review the details later that day before she approved payment.

Suddenly she noticed that a ransomware demand had appeared on her desktop. As the message appeared, it locked up the administrator's computer, and, within minutes, the entire network was down. She tried to access data files and realized that they had been encrypted and she could not access them at all. She spoke to other clinicians and staff who relayed that they, too, were not able to utilize their systems, and work had come to a standstill.

**In 2016, almost 80% of healthcare organizations suffered a data breach of some type.**

The administrator and the managing partner finally decided to utilize manual processes and paper charts, and not pay the ransom because they had backups of their files off-site. Backups were available (but only up to the previous night), and systems were restored the following day after several hours. That day the clerical and clinical staff spent time entering the manual data and clinical material into the systems in order to bring them current. The practice was able to resume normal operations on day 3 after the ransomware attack.

Unfortunately, there was no incident response protocol or contingency plan, so operations were disrupted for two days as the IT vendor sorted out the problems and restored the information via the backed-up files. The result was lost patient visits, staff overtime, and increased outsourced managed service provider costs. Periodic security risk training, regular updating policies and procedures, documenting incident response and contingency plans, and practicing "proactive threat intelligence" could have helped to prevent or mitigate the costs associated with this cybersecurity breach.

The IT vendor could not definitively determine which data were compromised or stolen, but the breach of over 5000 patient files caused the practice to notify both its patients and the Office of Civil Rights of the Department of Health and Human Services.

Technology has become more complex and more widely used in

*Continued on page 64*

*Cyber Secure* *(from page 63)*

healthcare. Data in electronic formats are ever more prevalent and are susceptible to loss or data breaches. Data security threats are increasing every day. And this doesn't include the thousands of security incidents that are never reported.

If you use, process, store, or transfer protected health information (PHI), security must be a top priority. You must ensure the security and privacy of PHI and fully comply with HIPAA, the Health Information Technology for Economic and Clinical Health Act, the Medicare Access and CHIP Reauthorization Act of 2015, and state-specific requirements. If you handle PHI, you should be performing periodic risk assessments, documenting and implementing security and privacy policies and procedures, conducting HIPAA awareness training, and regularly testing disaster recovery and business continuity plans.

You may ask: "Should I worry if I'm not secure and compliant? Could my business operations be disrupted by a data breach? Should I make the effort to perform a security risk assessment and implement required security processes and controls? Am I prepared if my customers and partners require me to be HIPAA compliant?" The answer to all of these should be an unqualified Yes.

Most smaller healthcare providers and business associates continue to believe that a security breach will not affect them. But the statistics are starting to say something totally different. The cause of data loss in healthcare organizations has changed drastically in recent years. In 2009, 80% of data loss was caused by theft and lost devices of all types. In 2016, hacking and unauthorized access caused over 75% of data breaches.

Ransomware attacks were up over 300% in 2016 and continue to rise. Also, in 2016, almost 80% of healthcare organizations suffered a data breach of some type. At the same time, the size and the cost of a data breach continue to rise.[1]

**The Dark Web**

The Dark Web, where individuals share malware, knowledge, and data anonymously, is growing rapidly. Small and medium-sized healthcare practices are becoming prime targets of hackers and opportunists. The risks are real, and they need to be managed. Here are just a few:

- Most small and medium-sized businesses have underspent on security.
- Healthcare records contain large amounts of personal information.
- Mass digitization of patient data has greatly increased attack opportunities.
- The value to thieves of a healthcare data record is 50 times that of a credit card record.
- Mobile devices have become the primary computing vehicle, increasing the potential for loss and theft.

Most small and medium-sized healthcare practices have similar security gaps. Do any of these sound like what your practice looks like?

- Incomplete or out-of-date risk assessment;
- Missing security and privacy policies and procedures;
- Limited or no security awareness training;
- Untested disaster recovery plans;
- Ad hoc data breach incident response;
- Inconsistent network monitoring; and
- Limited or no encryption of PHI.

Remediating security gaps and implementing basic security controls can pay dividends to your practice and also help you generate more revenue and increase new potential business opportunities. More and more business partners are asking if you are secure and HIPAA compliant. Many will not work with you if you cannot answer affirmatively to that simple question. Being secure can also be a business development differentiator; reduce the impact of a costly lawsuit over PHI mishandling or access; prevent reputational damage and consumer mistrust; and minimize potential fines from breaches and audits. It doesn't make sense for you to believe a data breach won't happen to you and gamble on your practice's well-being.

It doesn't have to be expensive. Several software solutions are available to guide your project and allow you to focus on only what you really need to do. This can make implementing strong security a cost-effective and potentially revenue-enhancing initiative. It can be completed in a few weeks with the appropriate level of effort and focus. So what steps should you take right now?

At a minimum, you should complete basic data security activities to minimize risks and be prepared to respond to business partners and new customer requests. This means completing at least the following steps:

- Perform a security risk assessment to understand where PHI is stored and used, identify critical technology risks that must be controlled, and establish what mitigating actions need to be taken.
- Perform a conduct gap analysis to prioritize remediation activities and develop a work plan to systematically close identified security gaps.
- Develop a work plan and strategy so progress can be measured and tracked.
- Remediate critical risks and implement mitigating controls to reduce risk and implement a secure and protected environment.

*Key activities include:*

- Developing and implementing security and privacy policies and procedures;
- Implementing ongoing monitoring tools to secure your technology, networks, and physical environments.

*Continued on page 65*

**The Dark Web, where individuals share malware, knowledge, and data anonymously, is growing rapidly.**

*Cyber Secure* *(from page 64)*

• Developing key risk management plans, including: incident response; contingency/business continuity; and physical security.

**Becoming secure and compliant doesn't have to be overwhelming or cost-prohibitive.**

• Performing ongoing vulnerability assessments of networks and devices to ensure that software and physical vulnerabilities are quickly identified and remediated.

• Conducting workforce training to ensure staff understand what security risks exist and what actions every staff member must do daily to maintain a secure environment.

In summary, the time for taking steps to secure your organization and PHI is now. Security needs to become a priority. Healthcare practices are under the microscope of regulators such as the CMS, the Office of Civil Rights, and the Consumer Financial Protection Bureau, and must be able to demonstrate their data and physical security safeguard protocols. As business partners and consumers become ever more computer-savvy, and as large data breaches are announced on almost a daily basis, they are asking "is my personal healthcare information data secure, and do you follow good security and privacy practices?" Becoming secure and compliant doesn't have to be overwhelming or cost-prohibitive. The primary rationale for implementing cybersecurity safeguards is a business decision, and the data indicates that this investment will pay for itself many times over. Get ahead of the curve. Bottom line... It pays to be cyber secure! **PM**

## Reference

[1] HIMSS Analytics. HIMSS 2017 Conference.

**Dr. Hausfeld** is Chairman of the Board and CMO of BioFactura Inc.; President, Memory Care Communities LLC; Chairman and Founder of The Society of Physician Entrepreneurs. e-mail: jhausfeldmd@outlook.com.

**Robert Zimmerman** is CEO, QI Express, Executive Director, HTA Foundation. e-mail: rzimmerman@qiexpress.com.