MGMA
Medical Group Management Association®

Cybersecurity Action Steps for Medical Practices

Introduction

The global cyberattacks that occurred recently caused a great amount of concern not only for cybersecurity and IT professionals but also with medical practice leaders. A catastrophic loss of data could be devastating to a practice. The negative impact on an organization's reputation could lead to lost referrals, patients leaving the practice, as well as diminished staff morale. Unrecoverable clinical information could also significantly impact a physician's ability to deliver high-quality patient care.

According to reports submitted to the U.S. Department of Health and Human Service's Office for Civil Rights, more than 170 million Americans health records have been exposed since 2009. In 2016 there was a record number of breaches involving 500 or more patients, with more than 16 million exposed records. The report from the Identity Theft Resource Center in March of this revealed that more than 25% of all data breaches were from the healthcare sector, costing the industry more than $5 billion per year.

There are a number of reasons why the healthcare industry has been the victim of so much cybercrime and theft of medical records is so rampant. Medical records can very easily be converted into money, with thieves using this data to sell fake identities and enable medical identity theft. These records can also be leveraged for more "traditional" identity theft, as medical records very often contain the type of information permitting the opening of a credit card, bank account, or loan in the name of the victim. Most recently, cybercriminals have moved to employing ransomware to force healthcare organizations to pay them money to regain access to encrypted and compromised systems and data. As well, healthcare organizations, in general, have been less quick (and less able) to adopt cybersecurity policies and procedures that have been implemented in other sectors of the economy. Medical practices, for example, tend to have smaller security budgets and teams than banks or other financial services organizations.

Action Steps

As the threat of a cyberattack against healthcare organizations has escalated in recent years, practice leaders need to be particularly vigilant in taking the steps necessary to protect patient data and protect the practice itself. Steps practices can take to protect their systems include:

1. **Conduct a complete HIPAA Security Risk Assessment**. Required since 2005 when the HIPAA Security Rule went into effect, practices should perform this assessment leveraging available MGMA and HHS resources or contract with a qualified consultant to conduct one. The security assessment should review not only issues related to practice

use of the Internet and the potential of an external cyberattack, but also the organization's administrative, physical, and technical safeguards.

2. **Keep computer operating systems and antivirus software up-to-date**. Practice leaders should be particularly alert regarding computer systems that run with older versions of Windows software. Using an older version of an operating system, or using a version that has not been patched can make these systems extremely vulnerable to a cyberattack.

3. **Encrypt all files and systems that contain patient information**. Encryption programs can be applied to individual computer files or entire computer drives. Note that lost or stolen patient data that has been encrypted is not considered a breach under federal law.

4. **Deploy strong authentication**—healthcare systems should use multifactor authentication or other types of consumer security that are already ubiquitous in the U.S. financial services arena.

5. **Ensure that your business associates are protecting your data.** Practices that contract with a business associate to perform a function with their patient data (e.g., data analytics vendor) should ensure that these 3rd parties are putting in place adequate protections to protect against cyberattack. Similarly, practices need to be vigilant regarding the type of protocols put in place by their Internet and IT system vendors.

6. **Consider cyber insurance.** Many medical liability carriers are now offering cybersecurity insurance policies. Review these products for applicability to your organization and for what they do and do not cover.

7. **Require training for all practice staff**. Cybersecurity training should be administered to all clinical and administrative staff and good cyber "hygiene" practices should be spelled out in the employee handbook. Do not forget to include part-time or volunteer working in this training and consider a regular re-training schedule for all staff.

8. **Instruct all staff** not to open emails, attachments or links from unfamiliar senders and report suspicious messages to their internal IT team or external IT vendor immediately.

9. **Back up patient data.** Review your options with third-party data back-up vendors and strongly consider a secure, off-site data location.

10. **Conduct periodic penetration tests.** These tests, most often performed by third-party vendors could include everything from your firewalls and networks, to the web servers driving your websites and patient portals.