How to improve your cybersecurity practices

Protect your patients' health care records and data from viruses, hackers and other cyberattacks by improving the security of your network and computers.

Health care records are so valuable that attacks on health information technology (health IT) systems have increased 125 percent over the last five years.[1] In fact, stolen patient data can be worth up to 50 times more than a Social Security or credit card number due to the numerous types of fraud that can result from information contained in a medical record.[2]

Unfortunately, four out of five health care providers and payer executives say their health IT systems have been compromised by cyberattacks.[3]

While the Health Information Portability and Accountability Act of 1996 (HIPAA) security rule and the Electronic Health Record (EHR) Meaningful Use/ Advancing Care Information program both require physicians to conduct a security risk analysis, good health IT system hygiene goes beyond compliance with government regulation. Moreover, using certified EHR technology means that your EHR has certain security capabilities, but is not a guarantee of either legal compliance or robust protection.

Conduct a checkup

Discover the steps you should take today to improve your cybersecurity practices and implement improved safeguards.

Note: The materials on this page are provided for information purposes only. They are not intended as legal advice and do not guarantee compliance with any state or federal laws or regulations.

1. Encrypt and password-protect mobile devices, including cell phones, tablets and laptops. Fact: Over five million smartphones were lost or stolen in 2014.[4]
2. To protect against malicious software ("malware"), ensure that your software and computer and server operating systems are regularly patched and updated. Fact: As many as 85 percent of targeted attacks on computers are preventable.[5]
3. Install and update your anti-virus software. Fact: Nearly one million new pieces of malware are created each day.[6]
4. Create one Wi-Fi network for your practice and another for your patients (e.g., practice and practice guest). Use different passwords for each. Fact: Unauthorized access was the leading cause of security incidents in 2015.[7]
5. Create and enforce a workplace policy requiring strong passwords, using a mixture of letters, numbers and symbols. Fact: It takes automated software under 90 minutes to crack common, simple passwords.[8]

[1] Ponemon Institute, available at http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf. Accessed Nov. 27, 2017.

[2] HIMSS Analytics on behalf of Symantec, available at https://www.symantec.com/content/dam/symantec/docs/infographics/symantec-healthcare-it-security-risk-management-study-en.pdf.

[3] KPMG, available at https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf.

[4] Consumer Reports National Research Center, available at http://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm.

[5] U.S. Department of Homeland Security, available at https://www.us-cert.gov/ncas/alerts/TA15-119A.

[6] Symantec, available at https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

[7] IBM X-Force Research, available at http://public.dhe.ibm.com/common/ssi/ecm/se/en/sej03320usen/SEJ03320USEN.PDF.

[8] The University of Edinburgh, available at http://www.ed.ac.uk/information-services/computing/desktop-personal/information-security/protect-yourself/basic-protection/choosing-strong-passwords.