MedPro Group
a Berkshire Hathaway company

Risk Tips

PATIENT SAFETY & RISK SOLUTIONS

Using Technology-Based Safeguards to Prevent Security Breaches

Securing patients' electronic protected health information (ePHI) continues to be a top priority for healthcare organizations of all sizes. The need for vigilance in data security is emphasized by reports suggesting that a complete health record can fetch between $250 and $1,000 on the darknet.[1]

Ongoing cyberattacks attacks on healthcare systems only further illustrate the need for healthcare leaders and staff members to take proactive steps to prevent theft of patient information and other sensitive data.

As healthcare organizations devise their security strategies, they will want to make sure their approaches are "flexible and resilient to address threats that are likely to be constantly evolving and multi-pronged."[2]

The risk tips listed in this publication focus on technology-based strategies to prevent cyberattacks and protect patients' ePHI. For more information about physical safeguards for preventing data breaches, see MedPro's *Risk Tips: Using Physical Safeguards to Prevent Security Breaches*.

1

Conduct a security risk assessment to determine potential areas of vulnerability and to identify system and process gaps that compromise the privacy and security of ePHI and other proprietary information. (**Note:** The HIPAA Security Rule requires covered entities and their business associates to conduct risk assessments.[3])

2. Ensure that antivirus software and firewalls are properly installed on the organization's computer network and are up to date. Contractual arrangements with technology and security vendors should specify the security results the organization hopes to achieve with its systems.

3. Install password protection on all computers in the organization, and require users to establish strong passwords (i.e., passwords that have a minimum number of characters and require letters, numbers, and symbols) or passphrases.

4. Determine under what circumstances and how often you want to require system users to change their passwords. Although periodically changing passwords has long been considered a best practice, some guidance suggests it doesn't improve security and actually may compromise it.[4] All policies should comply with state and federal regulations.

5. Consider two-factor or multi-factor authentication technology for an added layer of protection at login. This method involves a password and at least one other identifying technique, such as an electronic identification card, key fob, or fingerprint recognition.

6. Ensure that the organization's computer operating systems, software applications, and network-connected devices are updated routinely and that security patches are installed when they become available.

7. Implement controls that block malicious websites or consider even stricter limitations, such as allowing access only to websites that are known to be secure (a process known as "whitelisting").

8 Restrict user permissions on systems to prevent employees from downloading and installing software. Permissions should align with the functionality and access employees need to perform their jobs.

9 Review the organization’s email security settings and spam filters to ensure the system is blocking emails with suspicious attachments and/or links.

10 Consider implementing software to restrict access to USB ports and removable devices, which can help prevent unauthorized copying of data and transfer of computer viruses.

11 Use encryption technology to protect stored and transmitted data. Consider anti-theft technology that can remotely delete or disable information from a device in the event of loss or theft.

12 Tailor employees’ access to computer systems and electronic health records based on their roles and responsibilities. Limit users who can log in to your network via a remote connection.

13 Enable system timeouts and record locks to prevent unauthorized access to patient data. Set a limit on how many times users can attempt to log in to the network before they are locked out of their accounts.

14

Back up system data to a separate server on a regular basis so it can be restored if an incident, such as a ransomware attack, occurs. Keep backup information in a secure, locked location — preferably offsite. (**Note:** Only public information should be sent via anonymous file transfer protocol.)

15

Provide education on, and raise awareness of, the organization's security policies and safeguards as well as best practices for cybersecurity and data protection. Conduct training during orientation and at least annually as part of in-service education. Develop written guidance to prevent loss and theft of patient information.

16

Report any suspicious activity, possible security breaches, or thefts (e.g., suspicious computer activity and missing records) to the appropriate authorities and organizations (e.g., law enforcement, the Office for Civil Rights, your professional liability company, etc.).

17

Have an incident response team in place, and conduct incident response drills to identify potential security and policy gaps. The team should periodically review the organization's incident response plan and procedures for handling cyberattacks, privacy violations, and other situations (such as physical theft or loss of data) that can result in data breaches.

Resources

For more information about safeguarding systems and protecting patient information, see MedPro's *Risk Resources: Cybersecurity*.

Endnotes

[1] Nadrag, P. (2021, January 26). *Industry voices — forget credit card numbers. Medical records are the hottest items on the dark web.* Fierce Healthcare. Retrieved from www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web

[2] American Hospital Association. (n.d.). Cybersecurity. Retrieved from www.aha.org/advocacy-issues/cybersecurity/cybersecurity.shtml

[3] The Office of the National Coordinator for Health Information Technology. (2018, December 19). Privacy, security, and HIPAA: Security risk assessment. Retrieved from www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

[4] Relias Media. (2018, March 1). *NIST provides guidance on HIPAA passwords.* Retrieved from www.reliasmedia.com/articles/142282-nist-provides-guidance-on-hipaa-passwords; Cranor, L. (2016, March 2). *Time to rethink mandatory password changes.* Federal Trade Commission. Retrieved from www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

This document does not constitute legal or medical advice and should not be construed as rules or establishing a standard of care. Because the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, please contact your attorney or other professional advisors if you have any questions related to your legal or medical obligations or rights, state or federal laws, contract interpretation, or other legal questions.

MedPro Group is the marketing name used to refer to the insurance operations of The Medical Protective Company, Princeton Insurance Company, PLICO, Inc. and MedPro RRG Risk Retention Group. All insurance products are underwritten and administered by these and other Berkshire Hathaway affiliates, including National Fire & Marine Insurance Company. Product availability is based upon business and/or regulatory approval and/or may differ among companies.