MedPro Group
a Berkshire Hathaway company

Checklist

Improving Cybersecurity in Healthcare Organizations

Cybersecurity is a top concern in healthcare as cyberattacks on the industry continue to trend upward and data breaches become increasingly common.[1] Healthcare organizations are a significant target for cybercriminals because of the amount of information they maintain and its value — estimates suggest that health records can garner as much as $1,000 on the dark web.[2]

The relentlessness of cyberattacks and the emerging use of artificial intelligence (AI) to facilitate malicious behavior stresses the need for hypervigilance in safeguarding healthcare systems and data. Failure to do so may have serious consequences, and even minor security lapses could lead to major breaches.

The following checklist offers high-level guidance and areas of focus for improving cybersecurity in healthcare settings. Although this tool is not all-inclusive, it offers organizations a basis for developing a strong security stance.[3]

	Yes	No
Organizational Culture		
Do organizational leaders champion a strong security culture and engage in cybersecurity planning and decision-making?	□	□
Is the importance of a strong security culture emphasized from the top down, rather than driven solely by your organization's information technology (IT) department?	□	□
Do organizational leaders model good cyber hygiene and share with employees the ways in which they participate in the organization's security culture?	□	□
Is cybersecurity included as a key component of your organization's overall strategic planning, budget, and enterprise risk management initiatives?	□	□

	Yes	No
Organizational Culture (continued)		
Does your organization have qualified and competent personnel to support cybersecurity efforts, such as a chief information security officer, HIPAA security officer, systems administrators, and cybersecurity systems analysts?	□	□
Organizational Policies and Procedures		
Does your organization conduct routine security risk assessments (as the HIPAA Security Rule requires) to determine areas of vulnerability and identify system and process gaps that compromise the privacy and security of electronic protected health information (ePHI) and other proprietary electronic data?	□	□
Are security risk assessments conducted at least annually or when significant changes occur in IT systems, staffing, workflows, operations, and/or regulations?	□	□
Does your organization use the results of security risk assessments to guide the development and implementation of remediation plans, starting with the most critical areas of vulnerability?	□	□
Has your organization developed written policies and procedures to prevent breaches of ePHI and other sensitive data? (Policies and procedures should comply with state and federal privacy and security laws.)	□	□
Has your organization identified and documented the types of protected and proprietary data it controls, how it's received, how it's stored, where it's stored, how it's used and maintained, and who has access to it?	□	□
Are credible security approaches and access controls used to secure your organization's networks, such as data encryption, firewalls, antivirus software, spam filters, multifactor authentication, lockouts, and more?	□	□
Does your organization routinely inventory all devices that can access its networks, including hardware, medical devices, and personal mobile devices?	□	□
Are security features and best practices implemented to secure devices that access organizational networks (e.g., security software, biometric authentication, and remote disabling)?	□	□

	Yes	No
Organizational Policies and Procedures (continued)		
Has your organization installed access controls (e.g., password protection, multifactor authentication, and lockouts) on all systems and devices that are used to retrieve or view ePHI and other sensitive information?	□	□
Does your organization have robust password policies that comply with security best practices (e.g., minimum character requirements; use of symbols, letters, and numbers; use of passphrases, etc.)?	□	□
Do employees' system permissions align with their job functions and the access they need to perform their jobs, and are they restricted beyond those requirements?	□	□
Has your organization assessed its IT processes and workflows to ensure they allow maximum security while also maintaining ease of use to prevent workarounds?	□	□
Are employees prohibited from downloading and installing software onto organizational systems unless it's a function of their role?	□	□
Does your organization have safeguards in place to prevent risky behaviors, such as uploading or downloading data to/from unapproved websites, plugging in unsecure devices, and copying data to external drives?	□	□
Has your organization implemented physical security policies and safeguards (e.g., cameras, alarms, file locks, door access codes, etc.) to prevent the theft of electronic devices that contain ePHI and other sensitive data?	□	□
Does your organization limit the amount of information that it publishes on publicly available webpages (e.g., staff directories, contact information, and organizational charts) to prevent cybercriminals from using that data to create targeted attacks?	□	□
Does your organization routinely update its computer operating systems, software applications, and network-connected devices, and are security patches immediately installed when they become available?	□	□
Does your organization perform due diligence evaluation of any vendors that are considered business associates under HIPAA or that will have access to confidential or sensitive information?	□	□

	Yes	No
Organizational Policies and Procedures (continued)		
Does your organization have systems and tools to accurately log security-related events (e.g., unauthorized access, login attempts, and authentication errors)?	□	□
Does your organization have a policy for monitoring and analyzing security systems and logs to identify suspicious and unusual activity?	□	□
Does your organization have a plan for responding to cybersecurity incidents and data breaches that includes guidance related to immediate response and containment, legal requirements, staff responsibilities, communication, documentation, and corrective actions?	□	□
Is an incident response team established, and does the team help plan and review the organization's response plans and procedures for handling cyberattacks, privacy violations, physical loss of data, etc.?	□	□
Does your organization regularly back up critical data to a secure offsite server so it can be quickly restored if a cyberattack occurs?	□	□
Does your organization have procedures in place to handle loss of systems, including its electronic health record system?	□	□
Education and Training		
Has your organization implemented a comprehensive cybersecurity training program for its workforce (including volunteers)?	□	□
Does training occur at least annually and whenever new technologies are implemented or new risks are identified?	□	□
Do educators consider various training formats and activities (e.g., online learning, workshops, role-playing, etc.) to keep individuals engaged and aware?	□	□
Does your organization's cybersecurity training program include education on:		
• Organizational security policies, procedures, and safeguards?	□	□
• Best practices for cybersecurity and data protection?	□	□
• Common cyberthreats (e.g., malware, ransomware, phishing, and supply chain attacks) and how to identify them?	□	□

	Yes	No
Education and Training (continued)		
• Common ways that data breaches occur?	□	□
• Risky online behaviors (e.g., clicking on pop-up ads, using the same password for multiple sites, opening email attachments from unknown sources, failing to sign out of shared computers, etc.)?	□	□
• The ways in which AI is making cyberattacks more difficult to detect?	□	□
• Possible consequences of cybersecurity lapses (e.g., loss of systems, interruptions to patient care and processes, financial losses, reputational damage, etc.)?	□	□
• Procedures for reporting known or suspected cyberattacks on the organization?	□	□
• Incident response protocols?	□	□
Are educational approaches and outreach tailored to address individual employee needs, knowledge gaps, and risky behaviors?	□	□
Does your organization run ongoing educational campaigns to raise awareness about cybersecurity using a variety of methods to engage the workforce (e.g., email reminders, intranet posts, videos and graphics, and contests)?	□	□
Does your organization run simulated cyberattacks as part of training to help staff members learn to identify suspicious activity?	□	□
Does your incident response team conduct period response drills to identify potential security lapses or process gaps?	□	□

Resource

For more information on this topic, see MedPro's *Risk Resources: Cybersecurity.*

Endnotes

[1] Adler, S. (2025, July 15). Healthcare data breach statistics. *HIPAA Journal.* Retrieved from www.hipaajournal.com/healthcare-data-breach-statistics/

[2] Takaham, E. (2024, February 25). Why health care has become a top target for cybercriminals. *The Seattle Times.* Retrieved from www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals/

[3] This checklist is based on information from the following sources: U.S. Department of Health and Human Services, Office for Civil Rights. (2019, July 22 [last reviewed]). *Guidance on risk analysis.* Retrieved from www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html; Arctic Wolf. (2020). *The healthcare cybersecurity checklist.* Retrieved from https://thwebsiteassets.blob.core.windows.net/assets/Arctic-Wolf-Healthcare-Cybersecurity-Checklist.pdf; Adler, S. (2025, April 8). HIPAA compliance checklist. *HIPAA Journal.* Retrieved from www.hipaajournal.com/hipaa-compliance-checklist/; ESET. (n.d.). *HIPAA security checklist for healthcare.* Retrieved from www.healthit.gov/sites/default/files/comments_upload/hipaa-security-checklist.pdf; Indian Health Service. (2017). *IHS HIPAA security checklist.* Retrieved from www.ihs.gov/sites/hipaa/themes/responsive2017/display_objects/documents/IHS_HIPAA_Security_Checklist.pdf; MedPro Group. (2024 [last updated]). *Risk Tips: Preventing security breaches with technology-based safeguards.* Retrieved from www.medpro.com/documents/10502/3667697/Using+Technology-Based+Safeguards+to+Prevent+Security+Breaches.pdf; MedPro Group (2024 [last updated]). *Risk Tips: Preventing security breaches with physical safeguards.* Retrieved from www.medpro.com/documents/10502/3667697/Using+Physical+Safeguards+to+Prevent+Security+Breaches.pdf; MedPro Group. (2024). *Risk Tips: Securing mobile devices in healthcare.* Retrieved from www.medpro.com/documents/10502/3667697/Risk+Tips_Securing+Mobile+Devices+in+Healthcare_MedPro+Group.pdf; Cascella, L. M. (2024). *Go phish: Strategies for proactively preventing phishing attacks.* MedPro Group. Retrieved from www.medpro.com/proactively-preventing-phishing-attacks; Cascella, L. M. (2024 [last updated]). *Password security best practices for healthcare organizations.* MedPro Group. Retrieved from www.medpro.com/password-security-best-practices-for-healthcare-organizations; Cascella, L. M. (2024 [last updated]). *15 ways healthcare organizations can build a strong security culture.* MedPro Group. Retrieved from www.medpro.com/building-a-strong-security-culture-healthcare; Cascella, L. M. (2025 [last updated]). *Strengthening the frontline: Cybersecurity training for healthcare workers.* Retrieved from www.medpro.com/cybersecurity-training-for-healthcare-workers

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 may differ among companies.