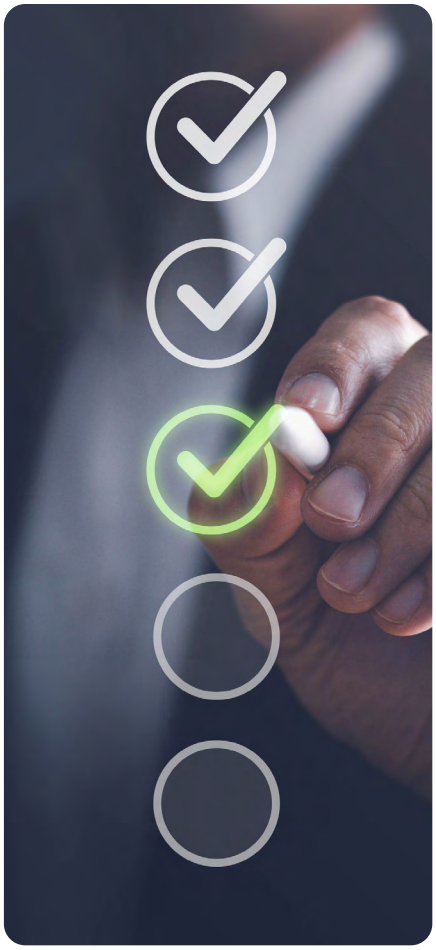
CloudWave

Healthcare IT Cybersecurity Checklist

This expanded checklist provides a comprehensive roadmap for elevating your healthcare IT cybersecurity posture, addressing both immediate priorities and long-term strategic goals.

Introduction



Cybersecurity in healthcare is no longer a matter of if, but when. Ransomware, data breaches, and third-party risks continue to rise, while regulators and insurers are placing new pressure on organizations to demonstrate active risk management. At the same time, healthcare systems are navigating IT complexity, clinical system dependencies, and staffing shortages—all of which create real barriers to effective cybersecurity.

In this environment, a strong healthcare cybersecurity strategy must incorporate more than compliance. It also needs to include a focus on protecting patients, preserving operations, and ensuring long-term resiliency. But knowing where to begin or how to elevate an existing program can be overwhelming. That's why CloudWave developed this *Healthcare IT Cybersecurity Checklist*. It provides a field-tested guide grounded in real-world healthcare environments, designed to help CISOs, IT leaders, and compliance teams identify gaps, set priorities, and take informed action.

Each section of this checklist aligns with high-impact areas like EDR, SOAR, vendor risk, and incident response planning—bringing together tactical advice and strategic goals. Whether you're just starting to build a modern healthcare cybersecurity program or looking to validate and mature your current efforts, this checklist gives you a solid framework for progress.

ENDPOINT DETECTION AND RESPONSE

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE

VENDOR RISK

INCIDENT RESPONSE PLANNING

1. Advance Beyond HIPAA/HITECH Compliance

- ☐ **Assess Cybersecurity Maturity:** Conduct a baseline assessment using frameworks like DOE C2M2, NIST-CSF or CIS Controls to identify your organization's current cybersecurity maturity level.
- ☐ **Set Aggressive Goals**: Develop a roadmap to achieve a higher maturity level within 12-18 months, focusing on proactive threat hunting, incident response automation, and endpoint protection.
- ☐ **Cost of Inaction:** Recognize that stagnant security practices may lead to higher cybersecurity insurance premiums or coverage denials. Quantify potential savings from improved security to justify investments.
- ☐ **Adopt Advanced Frameworks:** Transition to frameworks like NIST 800-53 or HITRUST for a more comprehensive security posture that exceeds HIPAA/HITECH requirements.
- ☐ **Staff Training:** Invest in regular cybersecurity awareness training for all employees, emphasizing phishing prevention and secure data handling.

2. Strengthen Vendor Security Management

- ☐ **Implement Robust Vendor Risk Management:** Block critical attack vectors by establishing a formal vendor risk management program. This includes regular assessments and audits of vendor security practices.
- ☐ **Document All Vendors:** Maintain a comprehensive inventory of all third-party vendors, including their roles, data access levels, and contact information.
- ☐ **Request and Review Security Practices:** Require vendors to submit detailed security policies, including encryption standards, incident response plans, and compliance certifications (e.g., SOC 2, ISO 27001).
- ☐ **Contractual Security Obligations:** Include cybersecurity clauses in vendor contracts, mandating regular security audits, breach notification timelines, and adherence to industry standards.
- ☐ **Continuous Monitoring:** Use tools to monitor vendor security posture in real-time, such as automated risk scoring platforms.

3. Enhance External Security Testing

- ☐ **Move Beyond Basic Vulnerability Scanning:** Standard scans are insufficient as botnets perform similar scans continuously. Implement advanced scanning tools that prioritize critical vulnerabilities.
- ☐ **Target External IPs:** Conduct thorough testing of all external-facing IP addresses, including cloud services, VPN endpoints, and remote access portals.
- ☐ **Grey-Box Penetration Testing:** Simulate real-world attacks by allowing testers partial knowledge of your environment. Whitelist pen-testers' IP addresses to bypass next-generation firewalls and assess internal network resilience.
- ☐ **Red Team Exercises:** Engage in red team-blue team simulations to test incident response capabilities and identify weaknesses in real-time.
- ☐ **Continuous Testing:** Shift to continuous or quarterly penetration testing to keep pace with evolving threats, rather than annual assessments.

4. Secure Single Sign-On (SSO) Deployments

- ☐ **Mandate Multi-Factor Authentication (MFA):** Ensure SSO is deployed with MFA across all access points to prevent unauthorized lateral movement within your environment.
- ☐ **Limit SSO Scope:** Restrict SSO to critical applications and segment access to sensitive systems to reduce the blast radius of a compromised SSO account.
- ☐ **Monitor SSO Activity:** Implement real-time monitoring and anomaly detection for SSO logins to identify suspicious behavior, such as logins from unusual locations.
- ☐ **Regular SSO Audits:** Conduct periodic audits of SSO configurations, user access levels, and integration points to ensure compliance with security policies.
- ☐ **Zero Trust Integration:** Incorporate SSO into a zero-trust architecture, requiring continuous verification of user identity and device health.

5. Transition from SIEM to SOAR

- ☐ **Understand SIEM Limitations:** A Security Information and Event Management (SIEM) system provides reporting and limited automation but often requires significant manual oversight. Assess whether your SIEM is adequately staffed or underutilized.
- ☐ **Adopt Security Orchestration, Automation, and Response (SOAR):** SOAR platforms automate repetitive tasks, integrate with threat intelligence feeds, and streamline incident response workflows, reducing reliance on manual processes.
- ☐ **Define SLAs:** Transition cybersecurity responsibilities into measurable Service Level Agreements (SLAs) using SOAR to ensure timely incident detection and response (e.g., 15-minute triage for critical alerts).
- ☐ **Staffing Optimization:** Evaluate whether your SIEM is managed by a dedicated team or a single employee. Use SOAR to offload routine tasks, allowing staff to focus on strategic initiatives.
- ☐ **Integration with Existing Tools:** Ensure your SOAR platform integrates with your SIEM, endpoint detection systems, and ticketing systems for a cohesive Security Operations Center (SOC) workflow.

6. Add Endpoint Detection and Response (EDR) to your SOC

- ☐ **Deploy EDR Solutions:** Install EDR tools on all endpoints to monitor, detect, and respond to advanced threats like ransomware and fileless malware.
- ☐ **Behavioral Analysis:** Use EDR platforms with machine learning capabilities to identify anomalous behavior, such as unusual process execution or network connections.
- ☐ **Centralized Management:** Consolidate EDR alerts into a centralized dashboard for real-time visibility and faster incident response.
- ☐ **Regular Updates:** Ensure EDR signatures and policies are updated frequently to address emerging threats.
- ☐ **Endpoint Hardening:** Combine EDR with endpoint hardening techniques, such as disabling unnecessary services and enforcing least privilege access.
- ☐ **Don't Use as a Standalone:** EDR and MDR (Managed Detection and Response) all roll up into a centralized SOC. If you're using them by themselves, you're not doing all you can, and are leaving valuable data underutilized.

7. Establish a Robust Incident Response Plan

- ☐ **Develop a Comprehensive Plan:** Create a detailed incident response plan that outlines roles, responsibilities, and procedures for handling cybersecurity incidents.
- ☐ **Tabletop Exercises:** Conduct regular tabletop exercises to simulate cyber incidents and test the effectiveness of your response plan.
- ☐ **External Partnerships:** Establish relationships with cybersecurity incident response firms and legal counsel to support major incidents.
- ☐ **Post-Incident Reviews:** After every incident, perform a root cause analysis and update the response plan to address identified gaps.
- ☐ **Communication Protocols:** Define clear communication channels for internal stakeholders, patients, and regulatory bodies during a breach.

8. Encrypt and Protect Sensitive Data

- ☐ **End-to-End Encryption:** Implement encryption for all sensitive data at rest and in transit, using strong algorithms like AES-256.
- ☐ **Data Classification:** Classify data based on sensitivity (e.g., CUI, PHI, PII) and apply appropriate access controls and encryption standards.
- ☐ **Key Management:** Use a secure key management system to store and rotate encryption keys, ensuring they are never hardcoded in applications.
- ☐ **Data Loss Prevention (DLP):** Deploy DLP tools to monitor and prevent unauthorized data exfiltration, especially for email and cloud storage.
- ☐ **Regular Backups:** Maintain encrypted, immutable, offsite backups of critical data and test restoration processes quarterly.

9. Foster a Security-First Culture

- ☐ **Leadership Buy-In:** Secure executive support for cybersecurity initiatives to ensure adequate funding and prioritization.
- ☐ **Employee Training Programs:** Roll out mandatory cybersecurity training programs, including simulations for phishing and social engineering attacks.
- ☐ **Reward Secure Behavior:** Incentivize employees to report security issues or participate in training through recognition or rewards programs.
- ☐ **Clear Policies:** Develop and communicate clear cybersecurity policies, including acceptable use of IT resources and consequences for non-compliance.
- ☐ **Regular Updates:** Keep staff informed about emerging threats and best practices through newsletters, town halls, or security awareness campaigns.

10. Monitor and Adapt to Emerging Threats

- ☐ **Threat Intelligence Feeds:** Subscribe to reputable threat intelligence services to stay informed about healthcare-specific threats, such as ransomware campaigns targeting hospitals.
- ☐ **Patch Management:** Implement a rigorous patch management program to address vulnerabilities in software and medical devices within 30 days of patch release.
- ☐ **Regulatory Compliance:** Stay updated on evolving regulations (e.g., OCR guidance, FDA cybersecurity requirements for medical devices) and adjust policies accordingly.
- ☐ **AI-Driven Threat Detection:** Explore AI-based tools for predictive threat detection and automated response to stay ahead of sophisticated attacks.
- ☐ **Industry Collaboration:** Participate in healthcare cybersecurity information-sharing groups, such as the Health Information Sharing and Analysis Center (H-ISAC), to learn from peers and share threat intelligence.

Closing Summary

While checklists are helpful, healthcare cybersecurity can't be solved with a series of static boxes to check. Every organization has different technologies, risk exposure, staffing resources, and compliance needs, and those variables change constantly. That's why a basic or overly generic checklist simply doesn't work for healthcare.

The CloudWave *Healthcare IT Cybersecurity Checklist* is meant to be a strategic guide—not a substitute for expertise or ongoing risk evaluation. It helps you identify blind spots and opportunities, but it's only the beginning. Real security comes from taking those insights and building a program tailored to your unique environment, threats, and regulatory pressures.

At CloudWave, we specialize in helping healthcare organizations turn planning into progress. Our cybersecurity experts, managed services, and advisory teams work with you to interpret, implement, and evolve your security strategy—without overextending your internal resources. Use this checklist to get started, but let us help you move from intent to execution.

Your patients, your reputation, and your future demand it.

CONTACT US →