

# Healthcare Cybersecurity Checklist

Your Guide Towards Cyber Preparedness & Resilience



## Elevate Your Cybersecurity Posture: A Strategic Guide for IT Risk Management

Healthcare security leaders face a wide range of vulnerabilities as they attempt to safeguard their organizations while also complying with regulations. Our checklist provides security teams with actionable steps to enhance cyber defenses.

Use this checklist to systematically review your current security measures, identify areas where security gaps exist, prioritize remediation tasks, and foster a culture of cybersecurity awareness.

### Data Protection

- Update Perimeter Controls & Firewall Rules: Review existing firewall rules to ensure they are up-to-date and aligned with the latest security policies.
- Review Network/System Inventory: Maintain accurate records of all assets.
- Review User Accounts: Verify proper permissions and least privilege access.
- Audit Elevated User Account Activities: Monitor high-risk accounts for unusual activity.
- Evaluate Mobile Device Management: Protect sensitive data on mobile devices.
- Generate Security Reports: Monitor systems for security events and threats.
- Review Security Audit Logs and Alerts: Maintain vigilance over system activities.
- Evaluate Maintenance Records: Ensure security is maintained during facility changes or repairs.
- Update Email, Spam, and Malware Filters: Protect against email-based threats.



### Incident Response

- Incident Response Testing: Validate effectiveness of response strategies.
- Evaluate Security Incidents: Analyze and learn from past incidents to prevent future occurrences.
- Review Anti-Virus Logs: Identify and respond to potential security threats.
- Monitor Failed Login Attempts: Detect and investigate unauthorized access attempts.



### Operations

- Review and Update Policies and Procedures: Include Business Continuity, Disaster Recovery, Incident Response, Risk Management plans, and Breach Notification plans.



## Physical Security

- Review Physical Badge Access: Ensure secure access to facilities.

## Resiliency

- Business Continuity and Disaster Recovery Testing: Ensure readiness for potential disruptions such as ransomware and other cyber-attacks.
- Test Backup Procedures: Ensure data can be recovered in case of loss.
- Assess Security Controls Post-Changes: Adapt security measures after environmental or operational changes.
- System Monitoring: Continuously oversee system health and security.

## Risk Management



- Review Business Associate Agreements: Ensure third parties comply with security standards.
- Conduct HIPAA Security Risk Assessment: Identify risks, gaps, and vulnerabilities to comply with federal regulations to safeguard patient information.
- Perform Third-Party Risk Assessments: Evaluate the security posture of all third-party vendors. Request and review the results of external audit results.
- Review and Update Risk Management Plans: Assess and update the risk management program, review remediation progress, and report results to management.
- Review Cybersecurity Insurance Coverage: Ensure comprehensive protection against cyber threats.
- Update Remediation Activities: Track and manage progress on risk mitigation.

## Training

- HIPAA Security Awareness Training: Educate staff on how to identify and report threats and vulnerabilities as well as security best practices and compliance requirements.
- Communicate HIPAA Security Reminders: Keep staff informed about security protocols.
- Phishing Training and Testing: Regularly educate employees to recognize and avoid phishing attempts.

## Vulnerability Management

- Perform External Vulnerability Scan/Penetration Test: Identify and mitigate security weaknesses in servers, networks, and applications.
- Update Firmware on Network Devices: Keep hardware secure with the latest updates.
- Patch Workstations and Servers: Address vulnerabilities promptly.



### Don't Let Complexity Compromise Your Security Posture With Intracorp Health

Cyberattacks put patients at risk and cost healthcare organizations millions. But with convoluted software systems and risk and vulnerability data lost in silos, leaders know their organization are vulnerable – and they feel little control over the safety of their patients, reputations, or bottom line.

Want to increase your cybersecurity resiliency while reducing vendor complexity? With Intracorp Health, you can ensure compliance, stay ahead of potential threats and protect your organization's future – without draining your resources.



**BOOK A CALL WITH AN EXPERT**

<https://intracorphealth.com/contact/>

## About Intracorp Health

Intracorp Health brings together cybersecurity experts with over 100 years of combined experience in healthcare to offer a comprehensive suite of innovative software and services. It helps leaders unlock a unified, human-centric cybersecurity approach by simplifying and unifying key healthcare cybersecurity assessments, prioritizing risks across complex organizations and vendor networks and accelerating remediation while saving staff time.