PLATOPS

Protect patient data and meet compliance

PlatOps provides security-first DevOps, cloud, and managed IT services for small and mid-sized businesses. We help organizations achieve compliance certifications, secure their infrastructure, and modernize their operations — without the enterprise price tag.

From SOC 2 and HIPAA compliance to cloud migrations and 24/7 monitoring, our team of engineers delivers measurable results with a 100% audit pass rate across 60+ client engagements.

100%	60+	8-12 wk	24/7
AUDIT PASS RATE	ORGANIZATIONS	AVG. TO COMPLIANCE	MONITORING

Healthcare Cybersecurity Checklist

Industry-Specific Security Controls for Healthcare Organizations

Prepared by PlatOps Security Version 1.0 | January 2026

HEALTHCARE THREAT LANDSCAPE

Why Healthcare is the #1 Target

The Perfect Storm:

1. **High-Value Data** - PHI sells for $250-$500 per record (vs $5-$10 for credit cards)
2. **Life-Critical Systems** - Organizations must pay to restore operations
3. **Complex Ecosystems** - Average hospital has 10,000+ connected devices
4. **Legacy Technology** - 73% of medical devices run outdated software
5. **Regulatory Pressure** - HIPAA requires breach disclosure

2024-2025 Healthcare Breach Statistics

METRIC	VALUE	TREND
Total Breaches	725	↑ 12%
Records Exposed	133M	↑ 15%
Ransomware Attacks	389	↑ 74%
Avg Ransom Demand	$1.5M	↑ 45%
Avg Days to Contain	553	↑ 15 days
Avg Breach Cost	$10.9M	↑ 9.8%

© 2026 PlatOps. All rights reserved. | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

VECTOR	PERCENTAGE
Phishing/Social Engineering	36%
Ransomware	28%
Third-Party/Supply Chain	18%
Insider Threats	12%
Unpatched Vulnerabilities	6%

PHI & PATIENT DATA PROTECTION

Electronic Health Records (EHR) Security (8 items)

- [ ] Encrypt EHR databases at rest (AES-256)
- [ ] Implement role-based access to patient records
- [ ] Enable audit logging for all PHI access
- [ ] Configure automatic session timeout (15 min max)
- [ ] Implement break-the-glass procedures for emergencies
- [ ] Secure EHR-to-EHR data exchange (HL7 FHIR security)
- [ ] Regular access reviews for clinical staff
- [ ] Integrate with identity provider (SSO/SAML)

Patient Portal Security (6 items)

- [ ] Enforce MFA for patient login
- [ ] Implement CAPTCHA and rate limiting
- [ ] Secure password reset process (no security questions)
- [ ] Encrypt all patient communications
- [ ] Implement consent management
- [ ] Regular penetration testing

Data Classification & Handling (6 items)

- [ ] Classify all data by sensitivity (PHI, PII, general)
- [ ] Label systems containing PHI
- [ ] Document data flows between systems
- [ ] Implement data loss prevention (DLP)
- [ ] Secure data disposal procedures
- [ ] Third-party data sharing agreements

Data Encryption Requirements (5 items)

- [ ] Encrypt PHI at rest on all systems
- [ ] Encrypt PHI in transit (TLS 1.2+)
- [ ] Encrypt backups
- [ ] Encrypt mobile devices and laptops
- [ ] Secure key management (HSM or cloud KMS)

© 2026 PlatOps. All rights reserved.

Internet of Medical Things (IoMT) Stats

STAT	VALUE
Connected devices per hospital bed	10-15
Devices with known vulnerabilities	53%
Devices running outdated OS	73%
Devices with default credentials	21%
Avg time to patch medical device	127 days

Medical Device Inventory (5 items)

- [ ] Maintain complete inventory of all medical devices
- [ ] Document network connectivity for each device
- [ ] Identify devices containing/accessing PHI
- [ ] Track software/firmware versions
- [ ] Assign risk classification to each device

Medical Device Security Controls (8 items)

- [ ] Segment medical devices on separate network
- [ ] Implement network access control (NAC)
- [ ] Disable unused ports and services
- [ ] Change default credentials on all devices
- [ ] Apply security patches within 30 days (where possible)
- [ ] Implement compensating controls for unpatchable devices
- [ ] Monitor device traffic for anomalies
- [ ] Establish vendor security requirements

Biomedical Equipment Management (4 items)

- [ ] Include security requirements in procurement
- [ ] Require vendor security assessments
- [ ] Document manufacturer patch support
- [ ] Plan for end-of-life device replacement

Medical Device Security Total: 17 items

© 2026 PlatOps. All rights reserved. | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

Telehealth Growth Stats

METRIC	VALUE
Telehealth visits growth	+38x since 2020
Patients using telehealth	76%
Physicians offering telehealth	85%
Security incidents in telehealth	+67%

Video Platform Security (6 items)

- [ ] Use HIPAA-compliant video platforms only
- [ ] Enable end-to-end encryption for video calls
- [ ] Require waiting room/host approval
- [ ] Disable recording unless consent obtained
- [ ] Implement meeting passwords
- [ ] Configure automatic meeting expiration

Patient Authentication (4 items)

- [ ] Verify patient identity before appointments
- [ ] Implement multi-factor authentication
- [ ] Secure password requirements
- [ ] Enable account lockout after failed attempts

Remote Care Security (5 items)

- [ ] Secure remote patient monitoring devices
- [ ] Encrypt data from wearables/sensors
- [ ] Implement secure data transmission
- [ ] Document consent for remote monitoring
- [ ] Regular security assessments of telehealth stack

Telehealth Security Total: 15 items

NETWORK & INFRASTRUCTURE SECURITY

Network Segmentation (5 items)

- [ ] Segment clinical network from administrative
- [ ] Isolate medical devices on separate VLANs
- [ ] Implement guest network for visitors
- [ ] Segment research/lab networks
- [ ] Document and regularly review firewall rules

Perimeter Security (5 items)

- [ ] Deploy next-generation firewalls

© 2026 PlatOps. All rights reserved.

- [ ] Enable DDoS protection

Endpoint Security (5 items)

- [ ] Deploy EDR on all endpoints
- [ ] Enable full-disk encryption
- [ ] Implement application whitelisting (clinical workstations)
- [ ] Configure USB device controls
- [ ] Maintain patch compliance (30-day window)

Wireless Security (4 items)

- [ ] Implement WPA3 or WPA2-Enterprise
- [ ] Segment wireless networks by function
- [ ] Conduct regular wireless penetration tests
- [ ] Monitor for rogue access points

Network Security Total: 19 items

ACCESS MANAGEMENT & IDENTITY

Identity Governance (6 items)

- [ ] Implement centralized identity management
- [ ] Configure single sign-on (SSO) for clinical apps
- [ ] Require MFA for all staff (clinical and admin)
- [ ] Implement privileged access management (PAM)
- [ ] Define role-based access control (RBAC)
- [ ] Automate provisioning/deprovisioning

Access Reviews (4 items)

- [ ] Conduct quarterly access reviews
- [ ] Review privileged accounts monthly
- [ ] Audit break-the-glass access usage
- [ ] Document access approval workflows

Termination Procedures (3 items)

- [ ] Revoke access within 24 hours of termination
- [ ] Collect physical badges and equipment
- [ ] Document termination in access logs

Access Management Total: 13 items

INCIDENT RESPONSE & RANSOMWARE

Healthcare-Specific IR Plan (6 items)

© 2026 PlatOps. All rights reserved.

- [ ] Establish media communication plan
- [ ] Document law enforcement engagement procedures

Ransomware Prevention (5 items)

- [ ] Implement immutable backups (3-2-1 rule)
- [ ] Test restoration procedures quarterly
- [ ] Block known ransomware file extensions
- [ ] Disable macro execution in email attachments
- [ ] Implement network segmentation to limit spread

Ransomware Response (4 items)

- [ ] Document ransomware-specific playbook
- [ ] Establish cryptocurrency wallet for potential payment
- [ ] Engage ransomware response retainer
- [ ] Document decision tree for ransom payment

Incident Response Total: 15 items

VENDOR & THIRD-PARTY RISK

Third-Party Risk Stats

STAT	VALUE
Breaches from third parties	40%
Vendors with PHI access	1,500+ (avg hospital)
Vendors assessed annually	23%

BAA & Vendor Management (5 items)

- [ ] Maintain vendor inventory with PHI access flags
- [ ] Execute BAAs before data sharing
- [ ] Include security requirements in contracts
- [ ] Track BAA renewal dates
- [ ] Document vendor termination procedures

Vendor Security Assessment (4 items)

- [ ] Require SOC 2 or equivalent from vendors
- [ ] Conduct security questionnaire assessments
- [ ] Review vendor security posture annually
- [ ] Monitor for vendor breaches (news, notifications)

Vendor Risk Total: 9 items

© 2026 PlatOps. All rights reserved. | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

Healthcare-Specific Training (6 items)

- [ ] HIPAA privacy and security training (annual)
- [ ] Role-specific PHI handling training
- [ ] Social engineering awareness
- [ ] Phishing simulation campaigns (monthly)
- [ ] Medical device security training
- [ ] Incident reporting procedures

Training Metrics to Track

METRIC	TARGET
Training completion rate	> 95%
Phishing click rate	< 5%
Phishing report rate	> 60%
Security incident reports	↑ 20% YoY

COMPLIANCE CROSSWALK

How This Checklist Maps to Frameworks

CONTROL AREA	HIPAA	HITECH	NIST CSF	HITRUST
PHI Protection	✓	✓	✓	✓
Medical Devices	✓	-	✓	✓
Telehealth	✓	✓	✓	✓
Network Security	✓	-	✓	✓
Access Management	✓	✓	✓	✓
Incident Response	✓	✓	✓	✓
Vendor Risk	✓	✓	✓	✓
Training	✓	✓	✓	✓

© 2026 PlatOps. All rights reserved. | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

Total Controls by Priority

PRIORITY	CONTROLS	TIMELINE
Critical (P1)	25	Immediate
High (P2)	30	30 days
Medium (P3)	20	90 days
Standard (P4)	10	6 months
TOTAL	**85**	

Controls by Category

CATEGORY	COUNT
PHI & Patient Data	25
Medical Devices	17
Telehealth	15
Network Security	19
Access Management	13
Incident Response	15
Vendor Risk	9
Training	6

Ready to Get Started?

Let our team of security and infrastructure experts help you achieve your goals faster.

100%	60+	8-12 wk	24/7
AUDIT PASS RATE	ORGANIZATIONS SERVED	AVG. TIME TO COMPLIANCE	MONITORING & SUPPORT

Get Free Assessment | Book Strategy Call | Healthcare Security Services

Email: hello@platops.com Phone: (202) 864-1197 Web: platops.com

This document is provided for informational purposes only. Requirements may vary based on your organization's specific circumstances. PlatOps is a registered trademark. Redistribution without permission is prohibited.