Your 90-Day HIPAA Security Checklist

Your EMR protects patient records within its digital walls effectively. Everything else, from the email your receptionist sends to the laptop your billing specialist takes home, exists outside that protection. These common gaps represent your true compliance challenge. How many do you have?

What needs to be managed

1. **Network Security**: Guest Wi-Fi without proper isolation exposes your entire network, while networked medical devices often run outdated firmware with known vulnerabilities.
2. **Endpoint Protection**: Lost and stolen devices continue driving breaches. The explosion of telehealth and remote work multiplied endpoints exponentially, with personal devices accessing patient data through various applications. Medical equipment running embedded Windows versions often lacks current security patches.
3. **Access Management**: Terminated employees retaining system access for weeks or months. Multi-factor authentication is not used on all systems, including email, file shares, and cloud storage.
4. **Email Security:** Standard email lacks encryption. Phishing attacks have grown sophisticated enough to fool experienced staff members. Employees using personal email for work convenience create shadow IT risks.
5. **Backup and Recovery**: Documentation of your disaster recovery process must meet specific HIPAA requirements for demonstrating data availability and integrity safeguards.
6. **Security Monitoring**: AI-powered security tools cut detection and containment time by weeks, reducing both impact and cost.
7. **Vendor Management**: Regular security assessments of key vendors identify risks before they become breaches.
8. **Physical Security**: Improper device disposal remains a consistent violation source. Server rooms require access restrictions. Workstation privacy filters, clean desk policies, and visitor management systems address risks.
9. **Human Factors**: Training gaps persist, particularly around automated encryption usage and recognizing sophisticated phishing attempts.

Your Action Checklist

Immediate Actions (Week 1-2):

- ☐ Enable multi-factor authentication on every system containing patient health information (PHI). Review access logs monthly.
- ☐ Review and revoke access for all terminated employees, including email, cloud storage, and building access.
- ☐ Switch to HIPAA-compliant encrypted email. Ban PHI in standard email
- ☐ Verify that your email encryption actually works by sending test messages and confirming recipients can access them properly.
- ☐ Schedule vendor Business Associate Agreement (BAA) audit.

SAGACENT® TECHNOLOGIES
Cybersecurity, IT Management & Compliance

SAGACENT® TECHNOLOGIES
Cybersecurity, IT Management & Cloud Solutions

Month 1 Priorities:

- ☐ Conduct a vendor audit, confirming current BAAs exist for every entity handling your PHI.
- ☐ Implement a backup testing schedule that includes actual restoration, not just verification.
- ☐ Deploy endpoint protection on all devices, including those personal devices accessing your network through personal devices.
- ☐ Launch first phishing simulation. Train staff quarterly on recognizing sophisticated phishing attempts.

Quarter 1 Initiatives:

- ☐ Segment your network to isolate medical devices and guest access from administrative systems.
- ☐ Schedule quarterly firmware updates for all network equipment.
- ☐ Roll out comprehensive security awareness training that addresses current threats, not generic HIPAA basics.
- ☐ Develop and test an incident response plan that everyone understands, with assigned roles from the front desk to the C-suite.
- ☐ Implement a 24/7 monitoring solution through managed services if internal resources are limited. Set alerts for unusual access patterns and large data exports. Review logs weekly at minimum.
- ☐ Schedule quarterly security training.

Further Actions:

- ☐ Test data restoration monthly, not just backup completion.
- ☐ Store backups in three locations including offsite.
- ☐ Audit every vendor handling PHI annually. Require proof of security practices, not just signed agreements. Include breach notification timelines in all contracts.
- ☐ Contract certified e-waste disposal with certificates of destruction.
- ☐ Install privacy screens on all monitors.
- ☐ Implement clean-desk policies with daily enforcement.

Secure Your Practice Today

Sagacent specializes in HIPAA security assessments that go beyond EMR compliance. We identify vulnerabilities across all nine zones and help implement solutions that fit your budget. Contact us for a confidential assessment, because $9.8 million is too much to gamble on incomplete compliance.

Contact Us

Phone: 408-248-9800 | Fax: 408-248-9700
Service: support@sagacent.com | Sales: sales@sagacent.com
Inquires: info@sagacent.com

SAGACENT® TECHNOLOGIES
Cybersecurity, IT Management & Compliance