Intraprise HEALTH

Cybersecurity Checklist: Your guide to better security

Empower your organization with a strong foundation of practical cybersecurity and compliance measures.

Our NIST-inspired HIPAA Security Checklist was designed as a guide to help organizations plan and prioritize HIPAA compliance and cybersecurity tasks. The checklist below is designed to help kickstart your cybersecurity planning and provides a guide to follow throughout the year.

Annual Checklist

- ☐ Perform an annual HIPAA security risk analysis per 45 CFR 164.308(a)(1)(ii)(A)
- ☐ Perform an annual external server and network vulnerability scan or penetration test (recommended at least quarterly but annual is absolute minimum.)
- ☐ Review policies and procedures (this assumes all policy, procedure, and plans are reviewed/updated to include BCP/DR, IR, Risk Management plans, etc. and that these documents are updated at the time)
- ☐ Conduct HIPAA security training
- ☐ Review perimeter controls and update firewall rules (ideally done every 6 months, but annual at a minimum)
- ☐ Conduct business continuity and disaster recovery testing
- ☐ Conduct incident response testing
- ☐ Review and update risk management plans (separate from risk analysis or assessment. This is more about reviewing the risk management program and updating the risks and threat factors used as part of assessments).
- ☐ Review security incidents
- ☐ Review business associate agreements
- ☐ Perform Third-Party Risk Assessments for all vendors
- ☐ Review and update existing cybersecurity insurance coverage

Quarterly Checklist

- ☐ Review network/system inventory to ensure accuracy
- ☐ Test backup procedures
- ☐ Review user accounts for terminated users, proper permissions, and least privilege access
- ☐ Audit and review elevated user account activities
- ☐ Review employee (or physical) badge access
- ☐ Review mobile device management (MDM)
- ☐ Update remediation activities

Monthly Checklist

- ☐ Update firmware on network devices
- ☐ Patch workstations, servers, mobile devices, etc.
- ☐ Generate security reporting from systems
- ☐ Review anti-virus logs for identification of security events and threats
- ☐ Review failed log-in log reports

Ongoing Activities

- ☐ Communicate HIPAA security reminders to staff
- ☐ As part of change management, evaluate security controls (technical and non-technical) after environmental or operational changes
- ☐ Review maintenance records and logs related to facility changes or repairs
- ☐ Perform system monitoring
- ☐ Review system security audit log reports and alerts
- ☐ Verify email, spam, content filtering, and malware updates are updated and applied on systems

The process to reduce risk doesn't happen overnight

Every organization needs a strong foundation of practical, simple, and effective security measures. To discuss your concerns and needs for your HIPAA or cybersecurity strategy, reach out to Intraprise Health to speak with a security and privacy compliance expert.

ABOUT INTRAPRISE HEALTH

Intraprise Health is an industry leading "tech-enabled" healthcare cybersecurity and risk management services provider. One of the longest tenured HITRUST Assessors in the industry, our broad range of information security, privacy and compliance services include: HITRUST Certification, Third-Party Risk Management, NIST Cybersecurity Framework Adoption, Advisory and Planning Services, Remediation Management, Incident Response and Business Continuity. We deliver HIPAA Security Risk Assessments and Workforce Training via our HIPAA One® platform. Our next generation BluePrint Protect™ platform, based on the NIST Risk Management Framework, provides intelligent monitoring, workflow management and collaboration capabilities.