HIPAA Security Rule Compliance Guide

CoreReconOS | HIPAA Security Rule — 45 CFR Part 164 Subpart C

Texas Healthcare | 18 Safeguards | OCR Enforcement Active

Texas Healthcare Threat Context

Texas healthcare attacks up 30% in Q4 2025. Change Healthcare / Ascension fallout drove unprecedented OCR scrutiny. BCBSTX subsidiary breach exposed 1.1M patient records.

$10.93M average healthcare breach cost (IBM 2024 Cost of a Data Breach Report). Texas is a top-3 state for healthcare data breach costs.

207-day median dwell time before detection — attackers spend months inside networks before being spotted.

Texas ranks among the top 3 states nationally for healthcare data breach costs per incident.

18 HIPAA Security Rule Safeguards

1. Security Management Process [Administrative]

Auditors look for: Written risk analysis, documented risk management plan, sanction policy for workforce members, system activity review logs
Common gaps: Risk analysis not updated annually, sanction policy absent or not distributed, no systematic information system activity review
Sentinel: Risk assessment engine, risk management tracking, automated sanction policy delivery, monthly activity review reports
Fortress adds: All Sentinel features plus quarterly risk re-evaluation, documented corrective action plans, continuous monitoring
Command delivers: All Fortress features plus enterprise risk management, board-level reporting, 6-year audit log retention for HIPAA compliance

2. Assigned Security Responsibility [Administrative]

Auditors look for: Designated security official in writing, contact info in policies, clear chain of responsibility
Common gaps: No named HIPAA security officer, responsibility assigned but not communicated, coverage gaps during absences
Sentinel: Named security officer designation, role documentation, coverage mapping for absences
Fortress adds: All Sentinel features plus backup officer documentation, responsibility communicated org-wide, Board-level visibility
Command delivers: All Fortress features plus DPO-as-a-service option, governance committee setup, annual responsibility review

3. Workforce Security [Administrative]

Auditors look for: Authorization procedures before granting access, supervision protocols, background checks for high-access roles
Common gaps: No formal authorization workflow, background checks not completed before access granted, supervision gaps for contractors
Sentinel: Role-based authorization workflows, access request tracking, background check tracking dashboard
Fortress adds: All Sentinel features plus automated provisioning/deprovisioning, supervision audit logs, contractor access reviews
Command delivers: All Fortress features plus identity governance integration, automated access certification campaigns, zero-trust architecture

4. Information Access Management [Administrative]

Auditors look for: Access authorization based on role, access agreements signed by workforce, policies for accessing ePHI
Common gaps: No role-based access matrix, access agreements missing or stale, overly broad access grants
Sentinel: Role-based access matrix, access agreement management, ePHI access logging, quarterly access reviews
Fortress adds: All Sentinel features plus automated access certification, segregation of duties controls, policy enforcement engine
Command delivers: All Fortress features plus advanced access governance, analytics-driven least-privilege enforcement, automated compliance reporting

5. Security Awareness and Training [Administrative]

Auditors look for: Annual security awareness training for all workforce, periodic reminders, malicious software training, login

monitoring, password management
Common gaps: Training completed but not documented, no phishing reminders, password policy not enforced, missing contractor training
Sentinel: Annual training program with documentation, monthly phishing reminders, password policy enforcement, training completion tracking
Fortress adds: All Sentinel features plus simulated phishing campaigns, role-specific training modules, breach scenario walkthroughs
Command delivers: All Fortress features plus gamified awareness platform, real-time threat briefings, executive tabletop exercises, compliance reporting

6. Security Incident Procedures [Administrative]

Auditors look for: Documented incident response plan, 24/7 response capability, incident logging, breach notification procedures
Common gaps: No formal IR plan, response capability untested, breach notification procedures not documented, no OCR reporting prep
Sentinel: IR plan documentation, incident classification framework, 24/7 alert monitoring, breach notification checklist
Fortress adds: All Sentinel features plus SOC-as-a-service, incident response playbook automation, OCR reporting template library
Command delivers: All Fortress features plus dedicated incident response team, ransomware-specific playbooks, HHS OCR notification support, post-incident reporting

7. Contingency Plan [Administrative]

Auditors look for: Data backup procedures, disaster recovery plan, emergency mode operations plan, annual contingency plan testing
Common gaps: Backups not tested, no documented disaster recovery plan, emergency mode plan missing, no annual testing
Sentinel: Automated backup scheduling, offsite backup storage, disaster recovery checklist, annual DR test documentation
Fortress adds: All Sentinel features plus cloud backup replication, DR runbook automation, failover testing, alternate site procedures
Command delivers: All Fortress features plus hot-site DR capability, annual DR exercise with documentation, executive continuity planning, BAA-covered cloud storage

8. Facility Access Controls [Physical]

Auditors look for: Contingency operations procedures, facility security plan, visitor access logs, maintenance records
Common gaps: No visitor log policy, no documented facility security plan, access controls not tested, maintenance records missing
Sentinel: Badge access control system, visitor log policy, facility security assessment, access log retention (6-year HIPAA requirement)
Fortress adds: All Sentinel features plus biometric access controls, CCTV integration, perimeter security hardening, maintenance scheduling
Command delivers: All Fortress features plus 24/7 physical security monitoring, SOC-affiliated guard services, integrated alarm systems, compliance reporting

9. Workstation Use [Physical]

Auditors look for: Written policy defining acceptable workstation use, location restrictions, proper workstation handling procedures
Common gaps: No written workstation use policy, location restrictions not communicated, policy not distributed to workforce
Sentinel: Workstation use policy template, policy distribution tracking, acceptable use agreement management
Fortress adds: All Sentinel features plus policy enforcement engine, endpoint lockdown capabilities, location-based access controls
Command delivers: All Fortress features plus advanced endpoint management, application allowlisting, comprehensive compliance reporting

10. Workstation Security [Physical]

Auditors look for: Physical safeguards for workstations, automatic logoff, screen lock policies, device placement standards
Common gaps: No automatic logoff configured, workstations in open areas, screen lock policies not enforced, no device placement standards
Sentinel: Automatic logoff configuration, screen lock enforcement, workstation physical security assessment, device placement guidelines
Fortress adds: All Sentinel features plus full-disk encryption enforcement, USB port controls, workstation hardening scripts, remote wipe capability
Command delivers: All Fortress features plus EDR integration, enterprise workstation management, advanced physical security controls, compliance verification

11. Device and Media Controls [Physical]

Auditors look for: Media disposal procedures, media re-use policy, accountability logs, data backup and storage procedures
Common gaps: No certified media destruction, accountability logs missing, data not purged before device re-use, backup tapes unencrypted

Sentinel: Certified media destruction vendor coordination, accountability logging, backup encryption (AES-256), media re-use policy
Fortress adds: All Sentinel features plus electronic media sanitization, backup media management, accountability reporting, BAA-covered storage
Command delivers: All Fortress features plus cloud-based media lifecycle management, automated backup verification, secure data destruction certification

12. Access Control [Technical]

Auditors look for: Unique user identification, emergency access procedure, automatic logoff, encryption/decryption of ePHI
Common gaps: Shared logins, no emergency access procedure documented, automatic logoff not configured, unencrypted ePHI at rest
Sentinel: Unique ID enforcement per user, MFA deployment, automatic logoff configuration, AES-256 encryption for ePHI at rest
Fortress adds: All Sentinel features plus single sign-on integration, emergency access procedure automation, contextual access controls, TLS 1.2+ for ePHI in transit
Command delivers: All Fortress features plus zero-trust network access, behavioral analytics, advanced threat detection, continuous compliance monitoring

13. Audit Controls [Technical]

Auditors look for: Hardware and software audit trails, log retention for minimum 6 years, regular log review process, audit log protection
Common gaps: Insufficient log retention (< 6 years violates HIPAA), logs not reviewed regularly, audit trails not protected from tampering
Sentinel: Automated audit log collection, 6-year retention (HIPAA-required), syslog/CEF/JSON format support, monthly compliance reports
Fortress adds: All Sentinel features plus SIEM correlation engine, real-time alerting, log integrity protection (hash chaining), advanced threat detection
Command delivers: All Fortress features plus dedicated SIEM correlation rules for HIPAA, behavioral analytics, executive compliance dashboards, audit trail export

14. Integrity [Technical]

Auditors look for: Mechanism for authenticating ePHI, digital signature support, protection against unauthorized modification
Common gaps: No integrity checking on ePHI, digital signatures not implemented, no protection against unauthorized modification
Sentinel: File integrity monitoring for ePHI repositories, change detection alerts, hash verification, audit of modifications
Fortress adds: All Sentinel features plus digital signature capabilities, automated integrity verification, content integrity reports
Command delivers: All Fortress features plus blockchain-backed audit trail option, advanced integrity monitoring, compliance-grade timestamping

15. Transmission Security [Technical]

Auditors look for: Encryption for ePHI in transit (TLS 1.2+), integrity controls on transmissions, transmission logging
Common gaps: ePHI transmitted over unencrypted channels, no TLS enforcement, integrity controls not implemented, transmission logs missing
Sentinel: TLS 1.2+ enforcement for all ePHI transmissions, SSL/TLS inspection, integrity hash verification, transmission logging
Fortress adds: All Sentinel features plus private API endpoints for ePHI, certificate management, advanced transmission monitoring
Command delivers: All Fortress features plus mTLS implementation, hardware security module (HSM) option, advanced transmission analytics

16. Risk Analysis (§ 164.308(a)(1)) [Other]

Auditors look for: Comprehensive risk analysis of all ePHI systems, documented methodology, regular updates, risk prioritization
Common gaps: Risk analysis not conducted organization-wide, analysis not updated after changes, risks not prioritized, analysis not documented
Sentinel: Risk analysis framework, ePHI inventory, risk scoring methodology, annual risk reassessment with documentation
Fortress adds: All Sentinel features plus automated risk scanning, continuous risk monitoring, risk treatment planning, executive risk register
Command delivers: All Fortress features plus enterprise risk management platform, real-time risk intelligence, board-level risk reporting

17. Risk Management (§ 164.308(a)(5)) [Other]

Auditors look for: Documented risk management strategy, implementation of security measures, monitoring of risks over time
Common gaps: No formal risk management strategy, security measures not implemented based on risk analysis, no ongoing monitoring
Sentinel: Risk management plan documentation, security measure implementation tracking, quarterly risk reassessment, remediation tracking
Fortress adds: All Sentinel features plus automated security control deployment, continuous risk monitoring, KPI-based risk tracking

Command delivers: All Fortress features plus enterprise security governance, real-time risk dashboard, integrated compliance management

18. Evaluation (§ 164.312(a)(2)(i)) [Other]

Auditors look for: Regular evaluations of security safeguards, documented evaluation process, remediation of findings
Common gaps: No regular evaluations conducted, evaluation results not documented, findings not remediated, no evaluation schedule
Sentinel: Annual evaluation program, compliance self-assessment toolkit, evaluation documentation, findings tracking dashboard
Fortress adds: All Sentinel features plus quarterly compliance evaluations, third-party assessment coordination, remediation project management
Command delivers: All Fortress features plus continuous compliance monitoring, OCR-audit-ready evidence packages, board-level evaluation reporting

HHS OCR Enforcement

Settlement trends: Anthem $16M, Premera $30M. Ransomware = breach unless proven otherwise. 60-day notification clock (2024 unified rule). OCR audit program active — small providers not exempt.

John Martinez
CEO & Founder, CoreReconOS
AT&T Vendor for State of Texas Incident Response | SDVOSB Certified
corerecon@polsia.app | corerecon.polsia.app