Apptega

GUIDE

HIPAA Security Rule Compliance Guide

(with NIST SP 800-66 Guidance)

Understanding and Implementing Security Requirements for Electronic Protected Health Information (ePHI)

Current as of August 19, 2025

Apptega

Apptega

1. Introduction

The HIPAA Security Rule requires covered entities and business associates to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI). This guide is a practical, implementation-focused playbook to become compliant. It defines owners, parameters, measurable acceptance criteria, evidence locations, and assessment mappings aligned to NIST SP 800-66.

1A. Beginner Quick-Start (First 30—90 Days)

Days 1—15 (Program stand-up & documentation skeleton)

- Appoint: Security Official, Privacy liaison, System Owner(s), IT/Cloud Owner, DR Lead, Third-Party Risk Lead.
- Define the ePHI authorization boundary; draft the ePHI data-flow map (systems, cloud services, vendors, interfaces).
- Build the Security Documentation Set skeleton: policy index, boundary narrative, role responsibilities, risk methodology, inheritance/shared-responsibility summary, and brief safeguard narratives.

Days 16—45 (Tailoring & full draft)

- Run safeguard workshops to confirm applicability, set parameters and acceptance criteria, and identify compensating controls.
- Establish identity/MFA, logging/alerting, encryption defaults, change control, and backup/restore baselines.
- Publish the first full Documentation Set by Day 45.

Days 46—90 (Evidence & readiness)

- Populate the Evidence Register; conduct one IR tabletop and one restore drill.
- Perform an internal assessment using 800-66 guidance; update the Documentation Set and the Remediation Log.
- Keep a versioned release of the Documentation Set for any external review.

2. Scope & Alignment

Scope. Include all people, processes, technology, and third parties that create, receive, maintain, or transmit ePHI. Cover on-premises and cloud systems (EHRs, billing, portals, data warehouses, analytics, integration engines, messaging, backups/DR sites), endpoints (workstations, mobile, medical devices that process/store ePHI), and interfaces (HIEs, clearinghouses, BA-managed services).

Foundations & Definitions

- **ePHI:** Individually identifiable health information in electronic form.
- **Reasonable and appropriate:** Tailor controls to risks, size, complexity, and capabilities.
- **Addressable vs. Required:** Addressable means implement or document an equivalent alternative with rationale in risk analysis.
- **Minimum Necessary:** Limit access/uses/disclosures to what's needed.
- **Business Associate (BA):** Vendor/sub-vendor that creates/receives/maintains/transmits ePHI on your behalf; requires a BAA defining security duties and incident notice.

Governance & Roles

- **Security Official:** Accountable for the Security Rule program and the Documentation Set.
- **System Owners:** Define use, acceptable risk, change approvals.
- **IT/Cloud Owner:** Operates identity, logging, network, endpoint, and cloud platform controls.
- **DR Lead:** Owns backup/restore, DR/BCP exercises, and evidence.
- **TPRM Lead:** Manages BAA portfolio, due diligence, and performance; validates inherited controls for cloud/services.

Environment Types & Handling

- **Secured clinical/office areas vs. controlled areas** (mixed-use). Apply physical controls proportionally and compensate with technical controls (encryption, device management, MFA).
- **Cloud & hosted services:** Treat as shared responsibility; document what you inherit and how service-level settings are verified (admin MFA, logging exports, encryption defaults, public access controls).
- **Portable/remote scenarios:** Enforce device management, encryption at rest, and encrypted channels; define remote access timeouts and restrictions.

Apptega

3. Safeguards & Practices (HIPAA Security Rule)

Each topic includes: Intent • Minimums • Implement (Procedural/Technical/Contractual) • Evidence • Acceptance Criteria • Common Failures • Internal QA Plan • Documentation tie-in.

AS1 — Security Management Process (§164.308(a)(1))

Intent: Manage risk to ePHI via risk analysis, risk management, sanction policy, and activity review.

Minimums: Documented risk analysis; prioritized treatment plan; sanctions for violations; routine system activity review.

Implement — Procedural: Annual (or change-triggered) risk analysis; risk register with owners/dates; sanction policy with HR; monitoring SOPs.

Implement — Technical: SIEM with admin/event logging; vulnerability scanning; baseline configs and drift monitoring; dashboards.

- **Evidence:** Risk analysis; risk register; sanction cases; SIEM reports; scan results.
- **Acceptance Criteria:** Risk analysis current and complete; top risks have owners/due dates; activity review executed on cadence with tracked findings.
- **Common Failures:** One-time RA; no linkage to remediation; incomplete scope.
- **Internal Audit Plan:** Trace five high-risk items from identification to closure.
- **Documentation tie-in:** Risk methodology, latest RA summary, treatment plan, activity-review SOP.

AS2 — Assigned Security Responsibility (§164.308(a)(2))

Intent: One accountable Security Official.

Minimums: Formal designation with authority/resources.

Implement: Charter; RACI; leadership reporting cadence; delegated admins with separation of duties.

- **Evidence:** Appointment letter; org chart; charter; meeting minutes.
- **Acceptance Criteria:** Authority documented; metrics reviewed quarterly.
- **Common Failures:** Title without authority; unclear decision rights.
- **Internal Audit Plan:** Interview Security Official; review last two governance meetings.
- **Documentation tie-in:** Role descriptions, delegation matrix, governance calendar.

AS3 — Workforce Security (§164.308(a)(3))

Intent: Authorize appropriate ePHI access and prevent inappropriate access.

Minimums: Authorization/supervision; workforce clearance; termination procedures.

Implement — Procedural: Joiner–Mover–Leaver ≤24h; role catalog; periodic re-screening for elevated roles.

Implement — Technical: SSO; group-based access; automated deprovisioning; badge disable sync; device wipe.

- **Evidence:** Access requests; clearance records; deprovision tickets.
- **Acceptance Criteria:** Deprovision ≤24h; orphaned accounts = 0; quarterly access recert ≥95% on time.
- **Common Failures:** Manual offboarding; shared accounts.
- **Internal Audit Plan:** Sample 10 hires/moves/exits.
- **Documentation tie-in:** JML procedure; access review SOP; clearance policy.

AS4 — Information Access Management (§164.308(a)(4))

Intent: Ensure minimum necessary access to ePHI.

Minimums: Policies for access authorization/establishment/modification; isolation of clearinghouse functions if applicable.

Implement: RBAC; least privilege; break-glass with approvals and auditing.

- **Evidence:** RBAC matrix; approvals; break-glass logs.
- **Acceptance Criteria:** All users mapped to roles; emergency access monitored; changes tracked.
- **Common Failures:** Ad-hoc privileges; stale service accounts.
- **Internal Audit Plan:** Sample 25 users + 10 admins.
- **Documentation tie-in:** Access authorization policy; break-glass SOP.

AS5 — Security Awareness & Training (§164.308(a)(5))

Intent: Workforce understands security responsibilities.

Minimums: Security reminders; malware protection; log-in monitoring; password management.

Implement: Role-based curriculum; phishing drills; developer secure coding; targeted refreshers after incidents.

- **Evidence:** Rosters; scores; phishing metrics.
- **Acceptance Criteria:** 100% trained before access; annual refresher; remediation ≤10 days.
- **Common Failures:** Generic training; no remediation.
- **Internal Audit Plan:** Trace 10 new hires + 10 role changes.
- **Documentation tie-in:** Training policy; curricula; tracking/report templates.

AS6 — Security Incident Procedures (§164.308(a)(6))

Intent: Respond to and report incidents impacting ePHI.

Minimums: Response and reporting procedures; evidence preservation.

Implement: Playbooks (phishing, ransomware, exfiltration, insider, vendor breach); escalation paths; forensics readiness; after-action reviews.

- **Evidence:** IR plan; tickets; artifacts; AARs.
- **Acceptance Criteria:** Tabletop within last 12 months; 24×7 contact path; corrective actions tracked.
- **Common Failures:** Delayed escalation; missing chain of custody.
- **Internal Audit Plan:** Review three incidents end-to-end.
- **Documentation tie-in:** IR plan, playbooks, comms matrix, evidence handling SOP.

AS7 — Contingency Plan (§164.308(a)(7))

Intent: Ensure availability of ePHI during emergencies.

Minimums: Data backup plan; disaster recovery; emergency mode operations; testing/revision; application/data criticality (addressable).

Implement: Recovery tiers and RTO/RPO; immutable backups; alternate compute; communication plan; quarterly restore tests.

- **Evidence:** Backup configs; test reports; DR runbooks; call trees.
- **Acceptance Criteria:** Quarterly restore tests hitting RTO/RPO; immutable copies ≥30 days; emergency mode procedures current.
- **Common Failures:** Unrestorable backups; co-located replicas.
- **Internal Audit Plan:** Observe one restore and review two test reports.
- **Documentation tie-in:** Backup policy, DR plan, emergency mode SOP.

AS8 — Evaluation (§164.308(a)(8))

Intent: Periodic technical/non-technical evaluation of security posture.

Minimums: Triggered by environmental/operational changes.

Implement: Annual evaluation plan; change-driven mini-evaluations; independent review when warranted.

- **Evidence:** Evaluation reports; action items.
- **Acceptance Criteria:** Evaluation(s) in the last 12 months or after major change; actions tracked to closure.
- **Common Failures:** Static posture; no follow-through.
- **Internal Audit Plan:** Confirm latest evaluation and mapped actions.
- **Documentation tie-in:** Evaluation plan and latest report.

AS9 — Business Associate Arrangements (§164.308(b))

Intent: Ensure BAs safeguard ePHI.

Minimums: Executed BAAs defining security obligations, incident notice, and downstream subcontractor flow-down.

Implement: TPRM intake; security due diligence; contract clauses (encryption, logging, breach notice timelines, right to audit); inheritance register.

- **Evidence:** Executed BAAs; due-diligence artifacts; monitoring records.
- **Acceptance Criteria:** 100% BAs under current BAA; obligations verified at onboarding and annually.
- **Common Failures:** Using MSAs without HIPAA terms; no subcontractor flow-down.
- **Internal Audit Plan:** Sample five BAs end-to-end.
- **Documentation tie-in:** BAA catalog and oversight procedure.

PS1 — Facility Access Controls (§164.310(a))

Intent: Limit physical access to facilities hosting ePHI systems.

Minimums: Contingency operations; security plan; access control/validation; maintenance records.

Implement: Badges/escorts; visitor logs; surveillance; environmental protections.

- **Evidence:** Access lists; logs; camera retention; maintenance records.
- **Acceptance Criteria:** Visitor logs retained; access validated quarterly; environmental tests current.
- **Common Failures:** Shared badges; uncontrolled deliveries.
- **Internal Audit Plan:** Walkthrough; sample logs.
- **Documentation tie-in:** Facility security plan; visitor management SOP.

PS2 — Workstation Use (§164.310(b))

Intent: Define secure workstation use.

Minimums: Proper functions, environment, and policies.

Implement: Screen lock; privacy screens; kiosk policies.

- **Evidence:** Policies; configuration baselines; spot-check reports.
- **Acceptance Criteria:** Timeouts in policy and enforced; privacy in sensitive areas.
- **Common Failures:** Kiosks without controls.
- **Internal Audit Plan:** Floor spot-checks.
- **Documentation tie-in:** Workstation use policy.

PS3 — Workstation Security (§164.310(c))

Intent: Physical safeguards for workstations.

Implement: Cable locks; secure placement; secure storage.

- **Evidence:** Photos; asset records.
- **Acceptance Criteria:** Critical workstations physically protected.
- **Internal Audit Plan:** Inspect 10% sample.
- **Documentation tie-in:** Workstation security standard.

PS4 — Device & Media Controls (§164.310(d))

Intent: Manage devices/media with ePHI.

Minimums: Disposal; media re-use; accountability (addressable); data backup and storage (addressable).

Implement: Chain of custody; certified destruction; crypto-erase; return-to-vendor process; removable media restrictions.

- **Evidence:** Media logs; destruction certificates; wipe reports.
- **Acceptance Criteria:** 100% tracked; 100% sanitized/disposed per policy; encryption on portable media.
- **Common Failures:** Lost drives; no proof of sanitization.
- **Internal Audit Plan:** Trace 10 items end-to-end.
- **Documentation tie-in:** Media control policy; destruction SOP.

TS1 — Access Control (§164.312(a))

Intent: Technical controls for unique access to ePHI.

Minimums: Unique user ID; emergency access; automatic logoff (addressable); encryption/decryption (addressable).

Implement: SSO; least privilege; break-glass; session timeouts; full-disk encryption on laptops; database/application encryption as risk-based.

- **Evidence:** Configs; logs; timeout settings.
- **Acceptance Criteria:** 100% unique IDs; emergency access logged/reviewed; timeouts enforced; encryption where risk warrants (documented rationale).
- **Common Failures:** Shared IDs; weak emergency access governance.
- **Internal Audit Plan:** Review 20 accounts; inspect break-glass records.
- **Documentation tie-in:** Access control standard; emergency access SOP.

TS2 — Audit Controls (§164.312(b))

Intent: Record and examine system activity.

Implement: Centralize logs; capture admin and ePHI access events; protect integrity/retention; alerting use-cases.

- **Evidence:** SIEM configs; event samples; retention settings; alert tickets.
- **Acceptance Criteria:** Required events on 100% systems; ingestion health monitored; alert triage SLA.
- **Common Failures:** Logging on but unused; no admin events.
- **Internal Audit Plan:** Validate five critical systems end-to-end.
- **Documentation tie-in:** Logging standard; alert response playbook.

TS3 — Integrity (§164.312(c))

Intent: Protect ePHI from improper alteration or destruction.

Minimums: Mechanism to authenticate ePHI (addressable).

Implement: Checksums/hashes; WORM/immutability for backups; application integrity checks; file integrity monitoring.

- **Evidence:** Configs; FIM coverage; immutability settings.
- **Acceptance Criteria:** Integrity controls documented and effective for critical stores/flows.
- **Common Failures:** No validation of export/import pathways.
- **Internal Audit Plan:** Verify integrity paths for three critical apps.
- **Documentation tie-in:** Data integrity standard; FIM procedure.

TS4 — Person or Entity Authentication (§164.312(d))

Intent: Verify identity of persons/entities accessing ePHI.

Implement: MFA for remote/admin; device certificates; service identity for APIs.

- **Evidence:** MFA coverage; cert inventories.
- **Acceptance Criteria:** 100% MFA on remote/admin; zero shared credentials.
- **Common Failures:** Unmanaged service accounts.
- **Internal Audit Plan:** Sample 10 service accounts; verify ownership and rotation.
- **Documentation tie-in:** Authentication standard; secrets management SOP.

TS5 — Transmission Security (§164.312(e))

Intent: Protect ePHI in transit.

Minimums: Integrity controls (addressable); encryption (addressable).

Implement: TLS 1.2+; secure email gateways; VPN/ZTNA; deny-by-default egress; approved file-transfer channels; message-level encryption where needed.

- **Evidence:** Cipher configs; email gateway settings; VPN configs.
- **Acceptance Criteria:** All ePHI flows use approved encrypted channels or justified alternatives; egress through managed interfaces.
- **Common Failures:** Legacy protocols; ad-hoc transfers.
- **Internal Audit Plan:** Map and test three representative data flows.
- **Documentation tie-in:** Transmission security standard; egress policy.

OR1 — Organizational Requirements (§164.314)

Intent: Contractually allocate security duties and ensure BA/sub-BA compliance.

Implement: BAAs with security terms; downstream flow-down; incident notice windows; audit/assistance obligations.

- **Evidence:** Executed BAAs; due-diligence records.
- **Acceptance Criteria:** 100% BAs with current BAAs; subcontractor flow-down verified.
- **Common Failures:** Informal agreements; stale terms.
- **Internal Audit Plan:** Sample three BA chains (prime → sub).
- **Documentation tie-in:** BAA template; vendor oversight procedure.

PD1 — Policies, Procedures & Documentation (§164.316)

Intent: Maintain written policies/procedures and proof of implementation.

Minimums: Documentation, availability, retention (≥6 years), and updates.

Implement: Policy library; version control; change log; staff access.

- **Evidence:** Policies; acknowledgments; revision history.
- **Acceptance Criteria:** Current policies accessible; changes tracked; retention met.
- **Common Failures:** Policy sprawl without version control.
- **Internal Audit Plan:** Check three policy updates for versioning and distribution.
- **Documentation tie-in:** Policy governance SOP; document control procedure.

4. Authorization Boundary & ePHI Data-Flow Mapping

Describe components, interfaces, trust zones, cloud services, external partners, and where ePHI flows, rests, and leaves. Maintain processing records (sources, stores, transmissions, recipients). Update on material change.

Documentation tie-in: Include diagram and narrative in the Security Documentation Set and keep synchronized during change.

5. Security Documentation Set — Canonical Narratives

Write cohesive narratives that prove how the program meets the Security Rule for the defined boundary: overview/mission; boundary & inventory; ePHI categories and lifecycle; roles/governance; inheritance/shared responsibility and verification; safeguard implementations; identity/MFA, zoning/egress, cryptography, logging, backups, vulnerability management; evaluation status and findings; change and baselines; vendors and sub-tiers. Keep versioned releases.

6. Applicability, Acceptance Criteria & 800-66 Mapping

Maintain a definitive record for each safeguard requirement: applicability, implementation summary, parameter values, measurable acceptance criteria, 800-66 task/objective mapping, inheritance type, and evidence link.

Illustrative excerpt:

Ref	Title	Applicable	Implementation Summary	Parameters	Acceptance Criteria	800-66 Map	Inheritance	Evidence
AS1	Security Mgmt Process	Y	Annual risk analysis; SIEM; vulnerability mgmt	Eval 12m; SLA H30/ M60	Current RA; top risks owned; activity review on cadence	T-1..T-6	System	Risk/RA_2025.pdf
TS1	Access Control	Y	SSO; least privilege; break-glass	Idle 15m; abs 12h	100% unique IDs; emergency access logged/reviewed	T-7..T-10	Hybrid	IAM/Access_Policy.pdf
TS5	Transmission Security	Y	TLS 1.2+; managed egress	Approvals for exceptions	All ePHI flows encrypted/ approved	T-11..T-12	Hybrid	Net/Egress_Rules.yaml
PS4	Device & Media	Y	Chain of custody; crypto-erase	Disposal SLA 30d	100% tracked & sanitized	T-13	System	Media/Destruction_Certs/

7. Control Parameter Defaults (Organization-Specific Settings)

- **Sessions & Access:** Idle 15 minutes; absolute 12 hours; failed attempts 5 within 30 minutes; lockout 30 minutes; emergency access monitored; privileged JIT elevation ≤60 minutes.
- **Cryptography:** TLS 1.2+ with strong suites; laptop full-disk encryption; server/database encryption based on risk; keys in KMS/HSM; key rotation 12 months.
- **Logging:** Required event set; ingestion health alerts daily; online availability ≥90 days; retention ≥12 months; time sync drift ≤5 minutes.
- **Patching & Vulnerability:** Critical ≤15 business days; High ≤30; Medium ≤60; Low ≤90; exceptions documented with compensating controls, expiry ≤90 days.
- **Backups & Recovery:** Daily incrementals; weekly full; immutability ≥30 days; quarterly restore tests meeting RTO/RPO.
- **Identity:** Deprovision ≤24 hours; no shared accounts; service accounts owned and rotated ≤90 days; phishing-resistant MFA for admin/remote where feasible.
- **Data Handling:** Approved export channels; labeling where needed; secure disposal ≤30 days after trigger; deny-by-default egress for ePHI flows.
- **Vendors:** Incident notice ≤72 hours; annual reassessment; subcontractor flow-down; right to audit for material services.

8. Evidence Register

Artifact	Safeguards	Location/Path	Owner	Format	Retention
Risk Analysis & Treatment Plan	AS1	Risk/RA_YYYY.pdf	Security Official	PDF	6 years
Access Recertification Qx	AS3/AS4/TS1	GRC/ Recerts/20YYQX	IAM Lead	CSV + approval PDF	6 years
MFA Coverage Report	TS4/TS1	IAM/Reports/MFA. csv	IAM Lead	CSV/PNG	3 years
SIEM Rule Pack & Health	TS2/AS1/AS6	SecOps/SIEM/	SecOps	JSON/PNG	Current + 1 year
Restore Drill Report	AS7	Resilience/Tests/ YYYY-MM	DR Lead	PDF	6 years
Firewall/Egress Ruleset	TS5	Net/Firewall/Ruleset. yaml	NetSec	YAML	Current + 1 year
BAA Catalog & Reviews	AS9/OR1	Legal/BAA/	Legal	XLSX/PDF	Active + 6 years
Training Roster & Results	AS5	L&D/Training/	L&D	CSV/PDF	6 years
IR Tabletop & AAR	AS6	IR/Exercises/YYYY	SecOps	PDF	6 years
Media Destruction Certs	PS4	Facilities/Media/	Facilities	PDF	6 years
Vulnerability Scan Results	AS1/TS3	VM/Reports/	SecOps	PDF/CSV	1 year
Policy Library & Revisions	PD1	Policy/Library/	Governance	PDF/MD	6 years

9. Continuous Monitoring Plan

- **Daily:** SIEM ingestion health; critical alerts triage; EDR/MFA coverage exceptions; backup job status.
- **Weekly:** Vulnerability scans; failed backups review; sample admin activity review; egress change review.
- **Monthly:** Access review roll-up; configuration drift review; patch SLA dashboard; vendor incident/vulnerability notices; BAA changes.
- **Automations:** Open tickets for ingestion failures, missing EDR/MFA, encryption drift, expired exceptions, failed backups, or BAA gaps.
- **Reporting:** Dashboards to Security Official; summary to leadership each quarter.

10. Remediation & Risk Acceptance Workflow

- **Workflow:** Identify → Record in the Remediation Log (severity, owner, due date, milestones) → Treat (remediate/compensate/time-bound accept) → Verify with evidence → Report.
- **Targets:** Critical ≤15 business days; High ≤30; Medium ≤60; Low ≤90.
- **Risk Acceptance:** Only with compensating controls, explicit expiry, leadership approval; reminder 14 days before expiry.
- **Registers:** Maintain a Risk Register (analysis, ratings, owners) and a Remediation Log (actions, status, evidence).

11. Cloud & Hosting (Shared Responsibility & BAAs)

Classify each safeguard as inherited, shared, or system-specific. Capture provider attestations, data locations, encryption/KMS model, logging/egress controls, incident notice SLAs, and subprocessor transparency. Verify service-level settings (admin MFA, log exports, storage encryption, public object defaults). Integrate SSO/MFA and SIEM exports. Reflect obligations in BAAs and due-diligence records.

12. Training & Awareness Program (Role-Based)

- **Tracks:** Workforce baseline; Admin/IT; Developers (secure coding/SDLC); Security Ops; Executives; Vendors with ePHI access.
- **Cadence & Metrics:** Onboarding before access; annual refresher; quarterly micro-modules; completion ≥98%; remediation ≤10 days; phishing failure rate trending down.
- **Artifacts:** Curricula, rosters, scores, phishing metrics, remedial coaching logs.

13. Vendor & Supply Chain Coverage (Business Associates)

Tier BAs that handle ePHI; set evidence expectations. Contract for security clauses; incident and vulnerability notice SLAs; encryption and logging requirements; subcontractor flow-down; right to audit. Monitor renewals, external attack surface, incident sharing, and change notifications. Offboard with data return/destruction and credential/certificate revocation; preserve logs.

14. SDLC Gatekeeping & Pipeline Controls

- **Plan:** Threat modeling; security non-functional requirements and acceptance criteria.
- **Build:** SAST/SCA; secrets scanning; artifact signing.
- **Test:** DAST; container and IaC scans.
- **Release:** Change approval; drift checks; rollout/backout plans.
- **Operate:** Observability; WAF/IDS; IaC drift monitors.
- **Blocking gates:** failing SAST/SCA/secrets/IaC checks block merge or release unless a time-bound exception with compensations is approved. Keep pipeline logs/signatures as evidence.

15. Evidence Sampling Plans (Internal Audit)

- **Access (AS3/AS4/TS1):** Sample 25 users and 10 admins; validate RBAC mapping, MFA status, last login, and deprovision proofs.
- **Changes (PD1/TS1/TS5):** Sample 10 change records; confirm approvals, PR reviews, rollback, and deployed state vs baseline.
- **Logging (TS2/AS1):** Sample 5 ePHI systems; verify required events, retention, and alert handling.
- **Backups/Restores (AS7):** Perform 3 restores from different tiers; confirm RTO/RPO.
- **Vulnerabilities (AS1/TS3):** Sample 20 hosts; verify patch SLA adherence and exception expiry.
- **Vendors (AS9/OR1):** Review 5 BAs; confirm BAA terms, logging/encryption assertions, incident notices, and subcontractor flow-down.

16. Common Pitfalls

- Assuming cloud “compliance” without verifying service-level settings.
- Missing parameter values (timeouts, cipher suites, lockouts) that make controls untestable.
- Logging turned on but unused (no alerting, no review cadence).
- Weak joiner–mover–leaver; shared admin credentials; unmanaged service accounts.
- Backups not restorable or stored with primary systems only.
- Vague BA agreements (no incident notice windows, no subcontractor flow-down).
- Evidence scattered; retention undefined.

17. Quick Reference Summary

Area	Core Artifacts	Examples
AS1	Risk analysis; treatment plan; SIEM dashboards	Vulnerability mgmt; activity review
AS2	Appointment letter; charter	RACI; governance minutes
AS3–AS4	RBAC matrix; access reviews; JML records	SSO; least privilege; break-glass
AS5	Training rosters; phishing metrics	Role-based tracks; remediation
AS6	IR plan; playbooks; AARs	Forensics readiness; comms matrix
AS7	DR plan; restore reports	Immutable backups; RTO/RPO
AS8	Evaluation plan & report	Change-triggered mini-reviews
AS9/OR1	BAA catalog; due diligence	Flow-down; audit rights
PS1–PS4	Visitor logs; maintenance; destruction certs	Facility/Workstation/Media controls
TS1–TS5	Access/crypto/logging standards; configs	MFA; SIEM; TLS/VPN
PD1	Policy library; revision log	Version control; acknowledgments

18. Self-Assessment & Leadership Attestation

Use status: **Compliant (C) / Partially Compliant (PC) / Not Compliant (NC) / Not Applicable (N/A).**

Tracker format (illustrative):

Safeguard	Status	Rationale (for N/A note inheritance/ scope)	Evidence Link	Owner	Action ID
TS1 – Access Control	C	—	IAM/Access_Policy.pdf	IAM Lead	—
TS4 – Authentication (Remote/Admin)	PC	—	IAM/MFA_Coverage.csv	IAM Lead	ACT-2025-017
TS2 – Admin Event Logging	NC	—	SecOps/SIEM/health.png	SecOps Mgr	ACT-2025-022
PS2 – Workstation Use (Kiosks)	N/A	No kiosks in boundary	Facilities/Scope.pdf	Facilities Sec	—

Attestation checklist: Inventory complete; each N/A has rationale and evidence; PC/NC items logged with owners/dates; contact paths current.

19. References & Resources

HIPAA Security Rule (45 CFR Part 164 Subparts A and C)
https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C

NIST SP 800-66 Rev. 2 — Implementing the HIPAA Security Rule
https://csrc.nist.gov/publications/detail/sp/800-66/rev-2/final

HHS OCR Security Rule Guidance Portal
https://www.hhs.gov/hipaa/for-professionals/security/index.html

HHS HIPAA for Professionals — Business Associates
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

National Vulnerability Database (NVD)
https://nvd.nist.gov/

National Checklist Program (Baseline Configuration Checklists)
https://nvd.nist.gov/ncp/repository

Apptega

Apptega Product Features

16+ Security Frameworks

One-Click Reporting

Automated Alerts & Notifications

API & Application Connectors

Automated Framework Crosswalking

Real-Time Compliance Scoring

Restricted Auditor View

Single Sign-On Connectivity

Policy & Plan Templates

Automated Risk Assessments

Document Repository for Artifacts

Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com