COMPLIANCE ALIGNMENT GUIDE

Total Access Control (TAC) and HIPAA

How TAC's architecture and capabilities support HIPAA Security Rule safeguards for protecting electronic Protected Health Information (ePHI) — for healthcare providers, payers, business associates, and the technology partners that serve them.

Audience	Regulation	Version
Healthcare CISOs, compliance leads, security architects	HIPAA Security Rule — Technical, Administrative, Physical Safeguards	v2.0 — 2026

Overview

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule establishes national standards for protecting electronic Protected Health Information (ePHI). Covered entities and business associates must implement **Administrative, Physical, and Technical safeguards** to ensure the confidentiality, integrity, and availability of ePHI.

Total Access Control (TAC) by PortSys directly addresses HIPAA's Technical Safeguards and several Administrative and Physical Safeguard requirements — particularly access control, audit controls, transmission security, and integrity controls. TAC's reverse-proxy architecture, built-in MFA, continuous device posture validation, and comprehensive audit trail provide defense-in-depth controls that map directly to HIPAA Security Rule requirements.

> **Note.** This guide describes how TAC's technical capabilities align to HIPAA Security Rule requirements under 45 CFR Part 164. HIPAA compliance is the responsibility of each covered entity and business associate. TAC is a technology platform that supports compliance — it is one component of a comprehensive HIPAA security programme that also includes policies, procedures, training, business associate agreements, and breach notification preparedness. PortSys recommends working with qualified healthcare compliance advisors.

Part A: HIPAA Technical Safeguards — § 164.312

TAC directly addresses all four Technical Safeguard standards and their implementation specifications. Each requirement below is matched to a specific TAC capability.

ACCESS CONTROL STANDARD

§ 164.312(a) — Access Control

REQUIREMENT	HOW TAC DELIVERS
§ 164.312(a)(1) Access Control (Standard)	TAC's reverse-proxy architecture ensures that ePHI-containing applications are never directly accessible from any network. Every access request passes through identity verification, multi-factor authentication, device posture validation, and policy evaluation before reaching the target application.
§ 164.312(a)(2)(i) Unique User Identification (Required)	Multi-directory identity federation connects to Active Directory, LDAP, SAML, RADIUS, OIDC, SQL databases, and custom directories — ensuring each user has a unique identifier. Both human and non-human (service account, AI agent) identities receive unique identification.
§ 164.312(a)(2)(ii) Emergency Access Procedure (Required)	TAC's policy engine supports emergency / break-glass access policies that can be activated when normal access procedures are disrupted, while maintaining full audit logging of every emergency-access event.
§ 164.312(a)(2)(iii) Automatic Logoff (Addressable)	Session timeout policies are configurable per application and user group. Continuous device posture validation can trigger automatic session termination if device compliance lapses mid-session.
Service accounts & AI agents	Non-human identities — service accounts, API clients, and AI agents accessing ePHI — governed by the same identity, policy, and audit framework as human users. No separate identity silo for programmatic access to ePHI.
§ 164.312(a)(2)(iv) Encryption and Decryption (Addressable)	All traffic to ePHI applications encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules. Single encrypted channel for all application access. No unencrypted protocols exposed.

AUDIT CONTROLS

§ 164.312(b) — Audit Controls

REQUIREMENT	HOW TAC DELIVERS
§ 164.312(b) Audit Controls (Standard)	TAC generates comprehensive audit logs for every access request, including: user identity, authentication method used, device posture status, source IP and geolocation, timestamp, application accessed, policy decision (allow / deny / step-up), and session duration. Logs cover both human users and AI agent access.
Native monitoring & SIEM export	Native real-time monitoring and alerting on access events. Optional SIEM export via syslog or API for downstream correlation, retention, and forensic analysis.
Information system activity review — § 164.308(a)(1)(ii)(D)	TAC provides the raw audit data required for HIPAA information system activity reviews. Reports cover access patterns by user, application, device, time period, and policy decision.

INTEGRITY CONTROLS

§ 164.312(c) — Integrity

REQUIREMENT	HOW TAC DELIVERS
§ 164.312(c)(1) Integrity (Standard)	TAC's reverse-proxy architecture mediates all connections between users and ePHI-containing applications. By preventing direct application access, TAC ensures that only authenticated, authorised, and policy-compliant users can reach protected data.
§ 164.312(c)(2) Mechanism to Authenticate ePHI (Addressable)	Built-in MFA with phishing-resistant FIDO2 / WebAuthn and six additional methods. Per-request policy evaluation ensures authentication is continuous, not just at initial login. Sessions can be revoked mid-flight when device compliance changes. Integrates with virtually any third-party MFA provider including Duo, RSA, Swivel, biometric solutions, and others.

PERSON OR ENTITY AUTHENTICATION

§ 164.312(d) — Person or Entity Authentication

REQUIREMENT	HOW TAC DELIVERS
§ 164.312(d) Person or Entity Authentication (Standard)	TAC provides robust authentication through: (1) multi-directory identity federation supporting seven directory types simultaneously; (2) built-in MFA with FIDO2 / WebAuthn, SafeLogin (proprietary), TOTP, push, SMS, OTP, and hardware tokens; (3) third-party MFA integration with virtually any provider; (4) continuous device posture validation as an additional authentication factor; (5) AI agent identity verification through certificate-based and API-key authentication. MFA enforced on all access **including legacy EHR and clinical applications** that cannot natively support modern authentication.
All MFA methods included in base licence	Built-in MFA methods and third-party integrations are all part of the base TAC licence — no add-on purchase, no per-user MFA surcharge, no premium tier. This eliminates the common HIPAA risk where organisations skip critical security controls because they are priced as premium add-ons.
Service account & AI agent authentication	Programmatic identities are authenticated and policy-evaluated on every request, just like human users. Service-account credentials and AI-agent identities are first-class citizens in the same policy framework.

TRANSMISSION SECURITY

§ 164.312(e) — Transmission Security

REQUIREMENT	HOW TAC DELIVERS
§ 164.312(e)(1) Transmission Security (Standard)	All ePHI transmissions are protected through TAC's single encrypted port architecture. Traffic is encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules — both between clients and the TAC reverse proxy, and between TAC and backend ePHI applications. Other inbound ports closed at the firewall.
§ 164.312(e)(2)(i) Integrity Controls (Addressable)	Reverse-proxy architecture terminates and re-establishes encrypted connections, enabling validation of traffic integrity without exposing ePHI to unencrypted network segments. TLS provides cryptographic message integrity end-to-end.
§ 164.312(e)(2)(ii) Encryption (Addressable)	End-to-end encryption between the user's device and TAC, and between TAC and the ePHI application. No clear-text ePHI traverses any network segment. All cryptography uses FIPS 140-2 compliant modules. No mechanism exists to access protected applications through unencrypted channels when TAC is deployed.

Part B: Administrative Safeguards Supported by TAC — § 164.308

TAC's technical capabilities support several Administrative Safeguard requirements through centralised policy management, comprehensive logging, and unified access control.

ADMINISTRATIVE SAFEGUARDS

§ 164.308 — Administrative Safeguards

REQUIREMENT	HOW TAC DELIVERS
§ 164.308(a)(1) Security Management Process	TAC's centralised policy management and comprehensive logging support risk analysis by providing visibility into who accesses what, when, from where, and with what device posture. Policy changes are versioned and audited.
§ 164.308(a)(3) Workforce Security	TAC enforces role-based and attribute-based access control, ensuring workforce members access only the ePHI systems authorised for their role. Termination procedures are simplified — revoking directory access immediately terminates TAC access across all protected applications.
§ 164.308(a)(4) Information Access Management	Unified policy engine provides centralised access authorisation. Access to ePHI systems is granted based on role, department, location, device compliance, and time — all managed from a single admin console.
§ 164.308(a)(5) Security Awareness and Training	TAC's audit logs provide visibility into access patterns that can inform security awareness training. Unusual access attempts — off-hours, unfamiliar locations, device posture failures — are logged for review by security teams.
§ 164.308(a)(7) Contingency Plan	TAC's Array and Global Array deployment models provide high availability and disaster recovery. A single SVA scales to Array (load-balanced HA within a region) and Global Array (worldwide active-active) to ensure continued access to ePHI during contingency events. 24×7 support included in base licence at no additional charge.

Part C: Physical Safeguards Supported by TAC — § 164.310

TAC's continuous device posture validation extends Physical Safeguard enforcement to every endpoint that accesses ePHI.

PHYSICAL SAFEGUARDS

§ 164.310 — Physical Safeguards

REQUIREMENT	HOW TAC DELIVERS
§ 164.310(b) Workstation Use	Continuous device posture validation ensures that only compliant workstations can access ePHI. Checks include OS version, patch level, antivirus status, disk encryption, firewall status, and domain join status.
§ 164.310(c) Workstation Security	Device posture policies can require specific security configurations (encryption, screen lock, endpoint protection) before granting access. Non-compliant devices are denied access in real time on every request, not just at login.
§ 164.310(d) Device and Media Controls	TAC's device posture validation serves as a continuous hardware and software inventory check for access-requesting devices. Geolocation restrictions can prevent access from unauthorised physical locations.

Why TAC Is Uniquely Strong for HIPAA Compliance

Close All Ports — Reduce the Attack Surface for ePHI

HIPAA requires reasonable safeguards to protect ePHI from unauthorised access. TAC's architecture closes all inbound firewall ports except one encrypted port (TLS 1.2 or TLS 1.3 with FIPS 140-2 modules), providing strong network-level protection for ePHI-containing systems. Most competing approaches leave datacenter ports open behind their cloud or concentrator — TAC closes them.

Single-Tenant Isolation for ePHI

Every TAC deployment is a dedicated, isolated Secure Virtual Appliance — on-premises, in your cloud account, or hybrid. Patient data from your organisation never co-mingles with another healthcare organisation's environment. This matters where shared-cloud architecture creates regulatory or board-level concerns.

Legacy Application Protection — Secure Every System with ePHI

Many healthcare organisations run critical ePHI systems on legacy applications that cannot natively support MFA or modern authentication. TAC's reverse-proxy architecture injects MFA, device posture checks, and continuous validation in front of any application — including thick-client EHR systems, forms-based portals, and legacy databases — without changing a single line of code or requiring clinical re-validation.

All-Inclusive Licensing — No Compliance Gaps from Budget Constraints

TAC includes every security feature in the base licence: all MFA methods, device posture validation, AI agent governance, SSO, and 24×7 support. No add-on tiers, no per-user MFA surcharges, no premium feature gates. This eliminates the common HIPAA risk where organisations skip critical security controls because they are priced as premium add-ons.

HIPAA Safeguard Coverage Summary

CONTROL FAMILY / FRAMEWORK	CONTROLS ADDRESSED	TAC COVERAGE
§ 164.312(a)	Technical — Access Control	Unique user ID, emergency access, auto logoff, service accounts & AI agents, encryption
§ 164.312(b)	Technical — Audit Controls	Comprehensive attributed audit trail, native real-time monitoring, optional SIEM export
§ 164.312(c)	Technical — Integrity	Reverse-proxy mediation, per-request authentication, mid-flight session revocation
§ 164.312(d)	Technical — Person or Entity Authentication	Multi-directory federation, built-in & third-party MFA, continuous device posture, AI agent auth
§ 164.312(e)	Technical — Transmission Security	TLS 1.2 / 1.3 with FIPS 140-2 modules, end-to-end encryption, integrity protection
§ 164.308	Administrative — Workforce & Access Management	RBAC / ABAC, centralised policy, immediate revocation, HA / DR via Array deployments
§ 164.310	Physical — Workstation & Device Controls	Continuous device posture validation, geolocation restrictions, real-time enforcement

Next Steps

Map your ePHI system inventory. Identify every application, database, integration, and AI agent that handles ePHI. Each is a candidate for TAC mediation.

Request a HIPAA compliance walkthrough. A PortSys healthcare specialist will walk through your specific environment, identify high-priority ePHI systems, and produce a prioritised deployment plan with timeline and milestones.

Contact: portsys.com/contact | info@portsys.com