Guardian Compliance, mapped to HIPAA

How PTS Guardian tiers cover the HIPAA Security Rule for medical, dental, and PHI-handling practices.

The business problem: HIPAA requires every Covered Entity and Business Associate to implement administrative, physical, and technical safeguards for protected health information (PHI). The Security Rule (45 CFR §§ 164.302-164.318) and the Breach Notification Rule (§§ 164.400-164.414) define those obligations. Most practices have the intent but not the documented controls, evidence, or program to prove it during an audit or after an incident.

The PTS answer: Guardian Compliance is our tier purpose-built for HIPAA-regulated practices. It combines our managed help desk, cybersecurity, backup, M365 E5 cloud, and vCIO management with the documentation, logging, and air-gapped recovery your auditor and cyber insurance carrier expect. **Compliance is the tier built to satisfy HIPAA end-to-end.**

THE SOLUTION

Why the Compliance tier

Compliance is the Guardian tier built end-to-end for HIPAA-regulated practices. Six capabilities make the difference between intent and audit-defensible evidence:

- **M365 E5 with Purview, DLP, and Message Encryption.** Native PHI data loss prevention, audit log retention, and encrypted external email. The controls auditors and OCR ask for.
- **SIEM with integrated compliance logging and network monitoring.** Satisfies §164.312(b) Audit Controls and the documented activity review requirement in §164.308(a)(1)(ii)(D).
- **Air-gapped monthly server backups, performed and tested by PTS.** Demonstrable §164.308(a)(7) contingency plan with monthly restore evidence. Defensible against ransomware and audit.
- **Annual incident response planning and 5-year IT lifecycle plan.** Documented program, not a one-time deliverable. Aligns with §164.316 and §164.308(a)(6).
- **Annual reorientation and full documentation refresh.** Policies, network diagrams, vendor inventory, and BA list stay current. The §164.316(b)(2)(iii) review requirement.
- **Employee productivity and access monitoring.** Activity review under §164.308(a)(1)(ii)(D) without ad-hoc spreadsheet tracking.

WHAT YOU GET

Inside the Compliance tier

A single managed-service bundle that delivers the help desk, security, backup, M365 E5 cloud, and vCIO management your HIPAA program depends on. Each layer is included in the monthly fee.

Service Layer	What you get
Help Desk	All remote, on-site, and emergency support within monthly limits. Acknowledge under 1 business hour, on-site under 8 business hours. 25% discount on after-hours emergency.
Cybersecurity	Advanced endpoint detection and response, 24/7 managed detection and response, phishing simulations and training, application allow-listing, DNS filtering, endpoint encryption, SIEM with compliance logging, network monitoring, employee productivity monitoring.
Backup	Image-based cloud backup (workstations and servers), 3x 2TB external drives included, monthly air-gapped server backups performed by PTS, monthly restore testing.
Cloud (M365 E5)	M365 E5 licensing, Purview audit logs, DLP, Message Encryption, email and file backup, DDoS protection, DNS and domain management.
vCIO Management	Quarterly TBR, PTS firewall/network/wireless standards, vendor management, 100+ policy templates, M365 hardening, white-glove MFA, annual incident response planning, 5-year IT and device lifecycle plan, annual reorientation and full documentation.

Why one bundle, not piecemeal tools

Most SMB practices end up with a patchwork: an MSP for help desk, a separate backup vendor, a security tool the office manager bought, and a compliance template purchased from a webinar. Guardian Compliance replaces that stack with one accountable provider.

What it takes	Piecemeal	Guardian Compliance
Vendor count	6 to 10 separate contracts: MSP, SOC, EDR, backup, M365, training	One contract, one invoice, one accountable provider
Documentation	Customer assembles policies and evidence from each tool	PTS maintains policy library, BAAs, and evidence binder
Restore testing	Backup vendor sells software; customer self-tests or skips	Monthly air-gapped restore performed and logged by PTS
Audit response	Practice scrambles to collect logs and policies from each vendor	One call to PTS, evidence delivered from existing binder
BAA accountability	Customer signs and tracks a BAA with every vendor independently	PTS is your Business Associate for the bundle, single BAA on file
Single point of escalation	Incident response routes through each vendor's separate support queue	P1-P4 escalation through one MSP, attorney-first protocol on day one

One contract. One BAA. One accountable provider. That is the difference between a tool stack and a HIPAA program.

THE PROOF

The cost of getting HIPAA wrong

Every breach affecting 500+ individuals is published on the public **OCR Breach Portal** (the "HIPAA Wall of Shame"). Settlements appear on the **HHS Resolution Agreements** page. Small practices are not exempt.

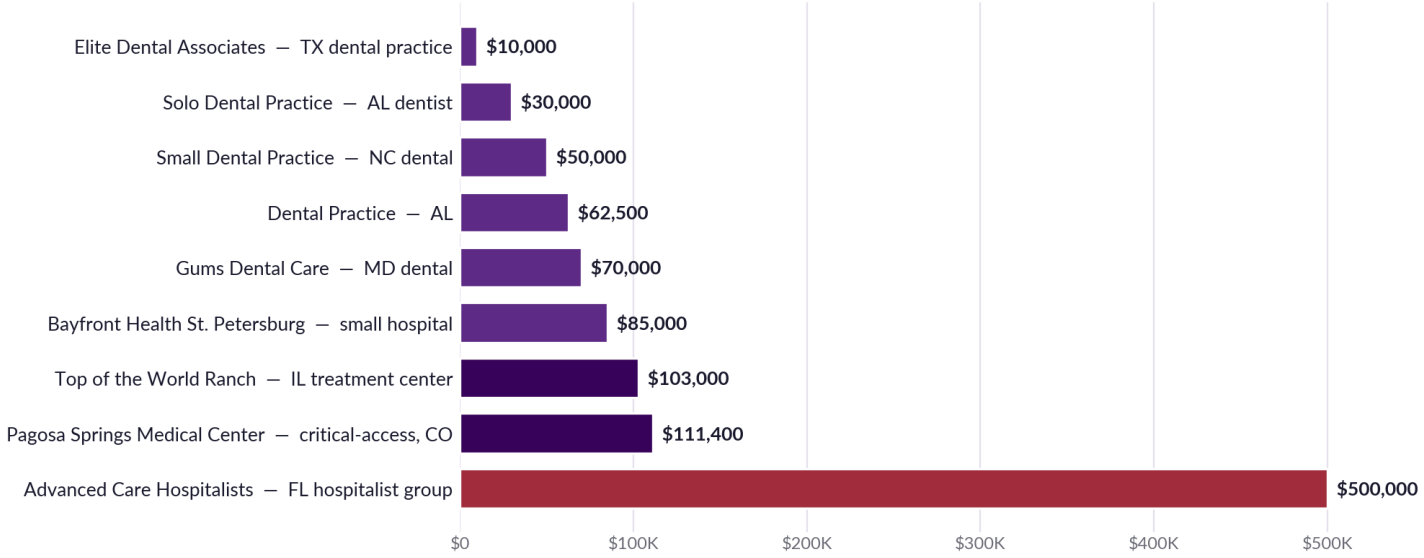
$1.5M
Annual maximum for a single category of willful-neglect violations

$50,000
Maximum per-violation penalty for willful neglect not corrected

6 years
Required retention for HIPAA policies, procedures, and breach documentation

60 days
Maximum window to notify affected individuals after a breach is discovered

Small practices pay too. And these are public record.



Beyond the settlement amount, every entity above also signed a multi-year Corrective Action Plan (CAP) requiring HHS oversight, mandatory risk analysis, policy rewrites, workforce training, and public reporting. The legal fees, breach notification costs, lost-patient revenue, and reputational damage typically exceed the fine itself by 5-10x.

Three patterns OCR keeps citing

Read across every resolution agreement on the HHS site and the same three findings repeat. Each is squarely inside the scope of a managed Guardian Compliance engagement.

PATTERN 01

No current Risk Analysis

The most cited failure across every settlement above. §164.308(a)(1)(ii)(A) requires a documented, dated risk analysis. Stale or missing is the same finding.

PATTERN 02

Lost or stolen unencrypted device

Laptops, USB drives, and backup tapes are the most common breach trigger for small practices. Full-disk encryption and inventory controls eliminate this exposure.

PATTERN 03

Failure to terminate access

Former employees with active EHR or M365 credentials surface in nearly every enforcement case. A documented joiner-mover-leaver workflow closes this gap.

THE DETAIL

Safeguard-by-safeguard mapping

Each row pairs a HIPAA Security Rule requirement with the Guardian capability that satisfies it, and shows which tier delivers it. Skim the Compliance column - every YES is a requirement covered out of the box.

ADMINISTRATIVE SAFEGUARDS §164.308

HIPAA §	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
§164.308(a)(1)	Security Management Process: risk analysis, risk management, sanction policy, information system activity review	vCIO/vCISO risk register, annual gap assessment, GRC-platform-driven remediation tracking, SIEM log review.	NO	PART	YES
§164.308(a)(2)	Assigned Security Responsibility: named Security Official	Guardian Compliance includes a designated PTS vCISO of record; named in your IRP and BAA.	NO	NO	YES
§164.308(a)(3)	Workforce Security: authorization, clearance, termination procedures	M365 identity hardening, JML (joiner/mover/leaver) workflow, Entra ID conditional access, documented offboarding.	NO	YES	YES
§164.308(a)(4)	Information Access Management: access authorization, establishment, modification	Role-based access in M365, application allow-listing, least-privilege baselines, quarterly access reviews.	NO	YES	YES
§164.308(a)(5)	Security Awareness and Training: security reminders, malware, login monitoring, password management	Monthly phishing simulations, ongoing security awareness training, enterprise password vault, dark web monitoring.	NO	YES	YES
§164.308(a)(6)	Security Incident Procedures: response and reporting	Documented Incident Response Plan, P1-P4 playbooks, 24/7 managed detection and response, partner SOC threat response.	NO	PART	YES
§164.308(a)(7)	Contingency Plan: data backup, disaster recovery, emergency mode operation, testing, criticality analysis	Image-based cloud backup, monthly air-gapped server backups performed by PTS, monthly restore testing, documented DR plan.	PART	PART	YES
§164.308(a)(8)	Evaluation: periodic technical and non-technical evaluation	Annual CIS Controls gap assessment, quarterly TBR with vCIO scorecard.	NO	PART	YES
§164.308(b)(1)	Business Associate Contracts: written assurances from BAs	PTS executes a HIPAA-compliant BAA; vendor management and BA inventory included in vCIO scope.	NO	YES	YES

PHYSICAL SAFEGUARDS §164.310

§164.310(a)(1)	Facility Access Controls: contingency operations, security plan, access validation, maintenance records	Documented facility access standards in policy library; physical security policy template; vendor visit log guidance.	NO	PART	YES
§164.310(b)-(c)	Workstation Use and Security: appropriate functions and physical safeguards	Acceptable Use Policy, workstation hardening baselines, screen-lock and idle-timeout enforced via Intune.	NO	YES	YES
§164.310(d)(1)	Device and Media Controls: disposal, media re-use, accountability, data backup and storage	Endpoint encryption, secure-wipe procedure for retired devices, documented media disposal log, encrypted external backup drives included.	NO	PART	YES

TECHNICAL SAFEGUARDS §164.312

§164.312(a)(1)	Access Control: unique user ID, emergency access, automatic logoff, encryption and decryption	M365 E5 identity, Entra ID conditional access, MFA/SSO, BitLocker endpoint encryption, automatic logoff via group policy.	PART	YES	YES
§164.312(b)	Audit Controls: hardware, software, procedural mechanisms to record and examine activity	SIEM with integrated compliance logging, Microsoft Purview audit log retention, network monitoring (Compliance tier only).	NO	NO	YES
§164.312(c)(1)	Integrity: protect ePHI from improper alteration or destruction	Immutable backups, file integrity monitoring, DLP via M365 E5, version control on document libraries.	NO	PART	YES
§164.312(d)	Person or Entity Authentication: verify identity before access	MFA enforced for all users (white-glove enablement), conditional access policies, password vault with rotation.	NO	YES	YES
§164.312(e)(1)	Transmission Security: integrity controls and encryption of ePHI in transit	TLS-enforced email, M365 Message Encryption, DNS web filtering, VPN/ZTNA where required.	NO	PART	YES

ORGANIZATIONAL, POLICIES & DOCUMENTATION §§164.314-164.316

§164.316(a)-(b)	Policies and Procedures and Documentation: written, retained 6 years, available to workforce, reviewed periodically	100+ policy templates including HIPAA-aligned set, secure documentation portal, 6-year retention, annual policy review cadence.	PART	YES	YES
§164.314(a)(1)	Business Associate Arrangements: written contract requirements	Standard PTS BAA; sub-processor list maintained; vendor risk reviews logged.	YES	YES	YES

BREACH NOTIFICATION RULE §§164.400-164.414

§164.404	Notification to Individuals: within 60 days of discovery	Documented breach notification workflow, attorney-first protocol, breach letter scaffold ready to deploy.	NO	PART	YES
§164.406	Notification to Media: for breaches affecting 500+ residents of a State	PR coordination playbook, OCR notification template, public statement framework.	NO	NO	YES
§164.408	Notification to the Secretary (HHS/OCR)	OCR breach portal submission included in IR retainer, Hiscox cyber insurance activation support.	NO	PART	YES
§164.410	Notification by a Business Associate	PTS-as-BA notifies you within contractual SLA; documented chain of custody and evidence preservation.	YES	YES	YES
§164.414	Burden of Proof: demonstrate notifications made (or low-probability-of-compromise risk assessment)	Forensic logs, audit trail, risk assessment documentation retained per §164.316.	NO	PART	YES

YES **Fully covered** **PART** **Partial / add-ons** **NO** **Not at this tier** | **Co-Mgd**: Co-Managed **Fund.**: Fundamentals **Compl.**: Compliance

THE PATH FORWARD

What working with PTS looks like

From first call to ongoing program: four clear stages, no surprises. Most practices complete Discovery and Assessment within two weeks and reach a deployed Compliance posture in 30-90 days.

1
Discovery
60-min HIPAA Readiness Review. We map your current environment against the safeguards in this document.

2
Assessment
Tenant health and CIS Controls gap assessment. You receive a one-page snapshot with prioritized findings.

3
Implementation
Guardian Compliance tier deployed in 30-90 days. M365 E5, SIEM, air-gapped backups, policies, training.

4
Ongoing
Quarterly TBR, monthly air-gap testing, annual reorientation. Optional vCISO layer for board-level depth.

Add a vCISO for governance depth

For practices facing an audit, a payer security questionnaire, a cyber insurance renewal, or a multi-location compliance program, a fractional **Phantom vCISO** engagement layers on board-level reporting, compliance roadmap, risk register ownership, and audit support. Tiers: Foundation (quarterly), Operational (monthly), Strategic (monthly plus on-call).

Common risk areas we find in SMB practices

- Missing or outdated Business Associate Agreements with software vendors
- No documented Security Risk Analysis in the last 12 months
- Backups exist, but restore testing has never been performed
- Former employees still hold credentials or EHR access
- PHI shared via unencrypted email or text
- No designated Security Official named in policies

Important. HIPAA compliance is achieved by the Covered Entity, not by any single vendor. PTS acts as your Business Associate and provides the technology, documentation, and program rigor that demonstrably support your safeguards under 45 CFR Part 164. Final policy adoption, workforce sanctions, and management attestation remain the responsibility of the practice.

Next step: 30-minute HIPAA Readiness Review

We walk your environment against this exact mapping and leave you with a one-page gap snapshot. No obligation.

Talk to PTS

hello@phantomts.com
phantomts.com/guardian

Why practices choose Phantom

Since 2010
OPERATING
Indiana-based MSP serving HIPAA-regulated practices, professional services, and SMB clients.

100+
POLICY TEMPLATES
HIPAA-aligned policy library maintained and applied to every Guardian Compliance engagement.

24/7
MDR COVERAGE
Partner SOC monitoring, incident response runbooks, attorney-first escalation.