eBOOK · HIPAA + SOC 2

Running HIPAA and SOC 2 Together: Overlaps, Gaps, and a Unified Control Set

Most health tech SaaS platforms need both. This guide maps overlapping controls and shows how to run both without doubling your compliance workload.

32 pages · PDF · Updated May 2026 · **goironfort.com**

Why Both?

Health tech SaaS companies often face a two-front compliance requirement: HIPAA (because they handle PHI) and SOC 2 (because their enterprise customers require it before signing contracts). Running these programs independently is expensive and redundant — roughly 60% of controls overlap.

Control Overlap Map

Control Area	HIPAA Reference	SOC 2 TSC	Shared Evidence
Access Controls	HIPAA §164.312(a)	SOC 2 CC6.1–CC6.3	MFA, unique user IDs, access provisioning/deprovisioning
Audit Logging	HIPAA §164.312(b)	SOC 2 CC7.2	Audit trails, log retention, log integrity
Encryption in Transit	HIPAA §164.312(e)	SOC 2 CC6.7	TLS 1.2+ for all ePHI/customer data transmissions
Encryption at Rest	HIPAA §164.312(a)(2)(iv)	SOC 2 CC6.1	AES-256 encryption for data at rest
Incident Response	HIPAA §164.308(a)(6)	SOC 2 CC7.3–CC7.5	IR plan, detection, containment, recovery, notification
Vendor Management	HIPAA BAA requirement	SOC 2 CC9.2	BA/vendor agreements, annual assessments
Risk Assessment	HIPAA §164.308(a)(1)	SOC 2 CC3.2	Annual risk analysis / risk assessment
Workforce Training	HIPAA §164.308(a)(5)	SOC 2 CC1.4	Security awareness training, role-based training
Backup & Recovery	HIPAA §164.308(a)(7)	SOC 2 A1.2–A1.3	Backup procedures, recovery time objectives
Policy & Procedures	HIPAA §164.316	SOC 2 CC5.3	Written information security policies and procedures

Gaps: HIPAA-Only and SOC 2-Only Requirements

HIPAA-only requirements (no SOC 2 overlap):

- Business Associate Agreements (BAAs) — required with every vendor handling PHI
- HIPAA Notice of Privacy Practices — required for covered entities
- PHI-specific breach notification to HHS and affected individuals
- Minimum Necessary standard for PHI access and use
- HIPAA Privacy Officer designation

SOC 2-only requirements (no HIPAA overlap):

- Trust Service Criteria coverage (Availability, Confidentiality, Processing Integrity, Privacy TSCs)
- Formal auditor opinion from a licensed CPA firm
- System Description document (management assertion)
- CC8.1 Change management controls with formal approval workflows
- Availability commitments (SLA documentation, uptime monitoring)

Unified Control Set Approach

The most efficient approach: build a unified control set that satisfies both frameworks, collect evidence once, and map it to both. Iron Fort does this automatically — every control implementation is tagged to both HIPAA and SOC 2 TSC references where they overlap.

> ■ *Organizations running HIPAA and SOC 2 through Iron Fort reduce total compliance effort by ~40% compared to running separate programs — because overlapping evidence is collected once and credited to both.*

Start Your Unified Compliance Program

Iron Fort's multi-framework module maps your controls across HIPAA and SOC 2 simultaneously. Book a free assessment at **goironfort.com/demo**.