ARTICLE · SOC 2 + HIPAA

Building a Modern Compliance Stack for Health Tech SaaS

A CTO's guide to the tools, integrations, and automation patterns that make continuous compliance achievable.

9 min read · PDF · Updated May 2026 · **goironfort.com**

In 2020, "compliance stack" meant a folder of Word documents and an annual consultant engagement. In 2026, it means automated evidence collection, continuous control monitoring, real-time alerts, and AI-powered gap analysis. This guide maps the tools and patterns that make continuous compliance achievable for a 20-person health tech team.

Layer 1: Identity & Access Management Foundation

Everything else in your compliance stack depends on knowing who has access to what. A solid IAM foundation covers single sign-on (SSO), MFA enforcement, user lifecycle management, and access review workflows.

Tool category requirements:

- SSO provider (Okta, Azure AD, Google Workspace) with MFA enforcement
- Automated user provisioning/deprovisioning integrated with HR systems
- Quarterly access review workflows with documented approval and exceptions
- Privileged access management (PAM) for production infrastructure

Layer 2: Infrastructure Security Monitoring

Continuous visibility into your cloud infrastructure configuration is the foundation of both HIPAA technical safeguard compliance and SOC 2 Common Criteria. Cloud security posture management (CSPM) tools identify misconfigurations in real time.

- Cloud-native security tools (AWS Security Hub, GCP SCC, Azure Defender)
- Vulnerability scanner (Tenable, Qualys, or AWS Inspector) with automated scheduling
- SIEM or log aggregation (Splunk, Datadog, Elastic) for audit trail centralization
- Endpoint detection & response (EDR) for workstations accessing ePHI

Layer 3: Compliance Automation Platform

This is where tools like Iron Fort sit — bridging your infrastructure security tools and your compliance frameworks. A compliance automation platform maps your existing controls to HIPAA/SOC 2/ITSG-33

requirements, collects evidence continuously, manages policies and vendor relationships, and tracks remediation.

> ■ *Health tech teams using a compliance automation platform spend 85% less time on evidence collection than teams using manual processes — and have significantly fewer audit findings because gaps are caught in real time rather than at pre-audit reviews.*

Layer 4: Vendor Risk & Contract Management

Every SaaS tool your team uses that touches customer data or ePHI is a compliance risk. Health tech companies average 47 SaaS applications with access to sensitive data. Your compliance stack must include systematic vendor assessment, SOC 2 / HIPAA certification tracking, and BAA/DPA management.

Layer 5: Policy & Workforce Governance

Policies that exist in SharePoint but haven't been reviewed in 3 years don't satisfy HIPAA or SOC 2. Modern compliance requires a policy management system with version control, approval workflows, annual review reminders, and workforce attestation tracking.

The Modern Health Tech Compliance Stack

Layer	Function	Example Tools
Layer 5	Policy & Workforce	Iron Fort Policies + Training
Layer 4	Vendor Risk	Iron Fort Vendor Risk Module
Layer 3	Compliance Automation	Iron Fort Platform
Layer 2	Infra Monitoring	AWS Security Hub / Datadog CSPM
Layer 1	Identity & Access	Okta / Azure AD with MFA

Iron Fort serves as the compliance automation layer — integrating with all other layers and maintaining your audit-ready posture continuously. Book a demo at **goironfort.com/demo**.