SOC 2 + HITRUST Implementation Readiness Checklist

Introduction

Digital health companies like CapMinds handle large volumes of electronic protected health information (ePHI) and patient-related data.

Protecting this data is essential to complying with regulations and maintaining patient trust. Two complementary frameworks help organisations demonstrate that commitment:

SOC 2 is an attestation framework developed by the American Institute of Certified Public Accountants (AICPA) for service organisations. SOC 2 auditors evaluate controls against five Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy. Only the security criterion is mandatory; the remaining four criteria are included based on the organisation's services and data practices. Each criterion has points of focus and control areas, such as control environment, communication, risk assessment, monitoring, access controls, system operations, change management, and risk mitigation.

HITRUST CSF (Common Security Framework) is a framework tailored for healthcare that is certified. It consolidates HIPAA, ISO 27001, NIST, and other standards into a single control set. HITRUST compliance matters because it helps healthcare organisations protect ePHI and demonstrate their commitment to security and privacy. The HITRUST readiness checklist covers domains such as building an information security program, endpoint protection, portable media and mobile-device security, configuration management, vulnerability management, network and transmission protection, access control, audit logging, training and awareness, third-party assurance, incident management, business continuity, risk management, physical and environmental security, and data protection & privacy.

Combining SOC 2 and HITRUST (often called SOC 2+ or HITRUST-mapped SOC 2) allows health-technology companies to satisfy multiple regulatory requirements within one control environment.

The following guide explains how to use the template and provides a comprehensive checklist that maps real-world tasks to both SOC 2 and HITRUST requirements.

How to Use This Template

Determine your scope and objectives

Identify which systems, services, and data flows will be included in your compliance program.
Select the Trust Services Criteria relevant to your services (security is mandatory; availability, processing integrity, confidentiality, and privacy are optional).
For HITRUST, define the business units, systems, and subsidiaries in scope and decide which assessment level (e1, i1, or r2) fits your needs.

Perform a readiness assessment

Conduct a gap assessment against the SOC 2 criteria and the HITRUST CSF. Evaluate existing controls and documentation, identify gaps, and prioritise remediation.
For HITRUST, ensure the scope is properly defined and assess documentation of policies and procedures against current HITRUST requirements.

Map controls to frameworks

Align your policies and operational procedures with SOC 2 requirements and document which controls support each Trust Services Criterion.
Likewise, map each control to the appropriate HITRUST domain (e.g., access control, configuration management, risk management).
Assign control owners and establish accountability.

Develop and formalise policies and procedures

Formalise core policies—such as access control, incident response, change management, and data classification—and ensure they are documented, enforced, and understood.
For HITRUST, establish an Information Security Management Program (ISMP) that outlines responsibilities and ethical values.

Collect and organise evidence

Gather audit logs, system configuration records, approvals, training records, and other evidence that demonstrates control operation.
Link evidence to the relevant SOC 2 and HITRUST controls.

Remediate identified gaps

Develop missing policies, modify workflows, train staff, and implement or improve technical controls (e.g., endpoint protection, change management, encryption) to close gaps.
HITRUST remediation should address gaps identified during the readiness phase and may take months, depending on the number of controls.

Conduct an internal review and readiness testing

Simulate auditor requests, verify policy enforcement and confirm that controls function as intended.
For SOC 2, performing a final readiness assessment before a formal audit helps ensure controls are working as designed.

Engage external auditors or assessors

Select a qualified CPA firm to perform your SOC 2 audit and an Authorized HITRUST Assessor for your HITRUST validation.
Share your readiness findings, schedule fieldwork, and cooperate during on-site assessments.

Maintain ongoing readiness

After obtaining your report(s) or certification, continuously monitor controls, update documentation, conduct annual training, and refresh risk assessments.
SOC 2 audits are typically annual, and HITRUST requires interim assessments for R2 certifications.

SOC 2 Readiness Checklist (All Criteria + Evidence)				
Category	**Control Area**	**What to Check**	**Status**	**Evidence Required**
Security (Required)	Access Control	RBAC implemented, MFA enforced, periodic access reviews	☐	Access logs, MFA config, user review logs
	Change Management	Documented change process, approvals, version control	☐	Change tickets, Git logs, approval records
	System Monitoring	SIEM logging, alerts configured, log retention	☐	Log samples, alert screenshots
	Risk Assessment	Annual assessment, risk register maintained	☐	Risk assessment report
	Incident Response	IR policy, response playbooks, escalation paths	☐	IR plan, post-incident reports
	Vendor Management	Vendor inventory, SOC reports collected	☐	VRA reports, SOC 2 reports from vendors
	Asset Management	Asset inventory, ownership, tagging	☐	Asset list export
	Secure Configuration	Baseline configs, hardened servers	☐	CIS benchmarks, config screenshots
	Data Security	Encryption at rest & in transit	☐	Encryption policy, cloud KMS config
Availability	Backup & Recovery	Backups configured, tested, DR plan updated	☐	Backup logs, DR test results
	Uptime Monitoring	SLA tracking, monitoring dashboards	☐	Uptime reports
	Failover Capability	Redundancy tested, auto-failover configured	☐	Failover test evidence
Processing Integrity	Data Accuracy	Validation rules, automated checks	☐	QA test cases, validation logs
	Error Handling	Retry logic, error detection	☐	Error logs
Confidentiality	Data Classification	Data labeled by sensitivity	☐	Classification policy
	Confidential Data Access	Access restricted, monitored	☐	Access logs
	Encryption	End-to-end encryption	☐	TLS certificates, KMS config
Privacy	Consent & Disclosure	Privacy policy, consent forms	☐	Policy docs
	User Rights	Right to access/delete implemented	☐	Ticket history

HITRUST Readiness Checklist			
Domain	**What to Validate**	**Status**	**Evidence Required**
Information Security Program	Policies documented, governance roles, annual review	☐	InfoSec policy, governance chart
Endpoint Protection	EDR/AV installed, patching, encryption	☐	Endpoint reports, patch logs
Portable Media Security	USB restrictions, encryption	☐	DLP logs
Mobile Device Security	MDM enrolled, remote wipe, password policies	☐	MDM dashboard
Wireless Security	Secure WiFi, segmentation, WPA2+	☐	WiFi config
Configuration Management	Baselines, change tracking, approval workflows	☐	Config baselines
Vulnerability Management	Monthly scans, remediation SLAs	☐	Scan reports
Network Protection	Firewall rules, segmentation, IDS/IPS	☐	Network diagrams
Transmission Protection	Data encrypted in transit (TLS 1.2+)	☐	SSL test reports
Password Management	Complexity rules, rotation, MFA	☐	IAM policy
Access Control	Least-privilege, JIT access	☐	Access logs
Logging & Monitoring	SIEM, log retention, audit trails	☐	SIEM export
Training & Awareness	Annual training, phishing tests	☐	Training records
Third-Party Assurance	Vendor assessments, contracts	☐	Vendor risk reports
Incident Management	IR plan, reporting workflow	☐	IR exercise reports
Business Continuity & DR	DR testing, BCP reviewed annually	☐	BCP/DR test results
Information Risk Management	Risk scoring & mitigation tracking	☐	Risk register
Physical Security	Access cards, CCTV, visitor logs	☐	Access badges, logs
Data Protection & Privacy	Retention, deletion, anonymization	☐	Data retention schedule

Evidence Collection Master Checklist

Evidence Type	Required Items	Status
Policies	Security, Access Control, IR, DR, Vendor Mgmt, Logging, Privacy	☐
System Records	Access logs, change logs, config backups, monitoring screenshots	☐
HR & Training	Background checks, onboarding records, training certificates	☐
Vendor Records	SOC 2 reports, BAAs, contracts, attestation forms	☐
Testing Evidence	DR test results, vulnerability scan reports, pen-test summary	☐
Architecture & Asset Docs	Network diagram, data-flow map, cloud architecture	☐

Final Audit Readiness Review		
Review Area	**Checklist**	**Status**
Control gaps remediated	Zero outstanding issues	☐
Evidence folder complete	All files labeled, dated, mapped to controls	☐
Stakeholders prepared	IR team, IT, DevOps, Security briefed	☐
Mock audit performed	Internal pre-assessment complete	☐