IHEP Security and Compliance Framework

NIST SP 800-53r5 Control Mapping & HIPAA Compliance

Document Classification: Security & Compliance - Confidential
Version: 1.1
Date: November 26, 2025
Compliance Frameworks: HIPAA, NIST SP 800-53r5, HITRUST CSF

Executive Summary

This document maps the Integrated Health Empowerment Program (IHEP) security architecture to NIST SP 800-53 Revision 5 controls and demonstrates comprehensive HIPAA compliance. Our security-first design achieves:

- **164 NIST controls fully implemented** (of 179 applicable controls = 91.6% coverage)
- **HIPAA Security Rule: 100% compliance** across Administrative, Physical, and Technical Safeguards
- **HITRUST CSF ready:** All critical requirements met for i1 certification
- **Zero Trust Architecture** with mathematical trust score validation
- **Continuous compliance monitoring** with automated auditing

1. HIPAA Security Rule Compliance Matrix

1.1 Administrative Safeguards

Standard	Implementation Specification	Status	IHEP Implementation	
164.308(a)(1)(i) Security Management Process	Required	✅ Implemented	Annual risk assessments using NIST 800-30 methodology. Risk register maintained in Jira. Quarterly reviews by security committee.	
164.308(a)(1)(ii)(A)	Risk Analysis	Required	✅ Implemented	Automated vulnerability scanning (Qualys), penetration testing (annual), threat modeling for all new features.
164.308(a)(1)(ii)(B)	Risk Management	Required	✅ Implemented	Risk treatment plans for all identified risks. Mitigation tracking in Jira with executive oversight.

Standard	Implementation Specification	Status	IHEP Implementation	
164.308(a)(1)(ii)(C)	Sanction Policy	Required	✅ Implemented	Employee handbook Section 12: Security violations result in progressive discipline up to termination. All incidents logged.
164.308(a)(1)(ii)(D)	Information System Activity Review	Required	✅ Implemented	Daily automated log analysis (Cloud Logging + BigQuery). Weekly security review meetings. Monthly executive reports.
164.308(a)(2) Assigned Security Responsibility	Required	✅ Implemented	Chief Security and Compliance Officer (CSCO) appointed. Reports to CEO. Security committee meets quarterly.	
164.308(a)(3)(i) Workforce Security	Required	✅ Implemented	Background checks for all employees. Role-based access provisioning. Annual security training.	
164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Addressable	✅ Implemented	Managers approve all access requests. Quarterly access reviews. Automated de-provisioning upon termination.
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Addressable	✅ Implemented	Security clearance levels (Public, Internal, Confidential, Restricted). PHI access requires HIPAA training + manager approval.
164.308(a)(3)(ii)(C)	Termination Procedures	Addressable	✅ Implemented	Automated workflow: HR termination triggers immediate access revocation across all systems within 15 minutes.
164.308(a)(4)(i) Information Access Management	Required	✅ Implemented	Role-Based Access Control (RBAC) with least privilege. Zero Trust architecture validates every request.	
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions	Addressable	N/A	IHEP is not a healthcare clearinghouse.

Standard	Implementation Specification	Status	IHEP Implementation	
164.308(a)(4)(ii)(B)	Access Authorization	Addressable	✅ Implemented	Formal access request process. Approved by manager + security review. Logged in immutable audit trail.
164.308(a)(4)(ii)(C)	Access Establishment and Modification	Addressable	✅ Implemented	Automated provisioning via Identity Platform. Changes require approval workflow. Quarterly access reviews.
164.308(a)(5)(i) Security Awareness and Training	Required	✅ Implemented	Annual HIPAA training (100% completion). Monthly phishing simulations. Security champions program.	
164.308(a)(5)(ii)(A)	Security Reminders	Addressable	✅ Implemented	Quarterly security newsletters. Slack security tips (weekly). Prominent security posters in offices.
164.308(a)(5)(ii)(B)	Protection from Malicious Software	Addressable	✅ Implemented	Endpoint protection (CrowdStrike). Email filtering (Proofpoint). Web filtering (Zscaler). Weekly malware briefings.
164.308(a)(5)(ii)(C)	Log-in Monitoring	Addressable	✅ Implemented	Failed login attempts logged. 5 failures = account lockout. Geographic anomaly detection. Weekly review.
164.308(a)(5)(ii)(D)	Password Management	Addressable	✅ Implemented	12+ character passwords. MFA required. Password manager provided (1Password). No password reuse policy.
164.308(a)(6)(i) Security Incident Procedures	Required	✅ Implemented	Incident response plan (IRP) documented. On-call rotation (PagerDuty). Quarterly tabletop exercises.	
164.308(a)(6)(ii)	Response and Reporting	Required	✅ Implemented	Incidents logged in ServiceNow. Breach notification procedure per 164.404. Post-incident reviews.

Standard	Implementation Specification	Status	IHEP Implementation	
164.308(a)(7)(i) Contingency Plan	Required	✅ Implemented	Business continuity plan (BCP) and disaster recovery plan (DRP). Tested annually. RTO: <1 hour. RPO: <15 minutes.	
164.308(a)(7)(ii)(A)	Data Backup Plan	Required	✅ Implemented	Automated daily backups (Cloud SQL, Healthcare API, Firestore). Cross-region replication. Quarterly restore tests.
164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Required	✅ Implemented	Multi-region architecture (primary: us-central1, secondary: us-east1). Automatic failover. Runbooks documented.
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Required	✅ Implemented	Manual workarounds documented for critical functions. Emergency access procedures. Satellite office backup.
164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Addressable	✅ Implemented	Annual DR test. Quarterly BCP tabletop. Plans updated within 30 days of major changes.
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Addressable	✅ Implemented	All applications rated (Tier 1: Critical, Tier 2: Important, Tier 3: Standard). RTOs/RPOs defined per tier.
164.308(a)(8) Evaluation	Required	✅ Implemented	Annual third-party security assessment. Quarterly internal audits. Continuous automated compliance monitoring.	

1.2 Physical Safeguards

Standard	Implementation Specification	Status	IHEP Implementation	
164.310(a)(1) Facility Access Controls	Required	✅ Implemented	Cloud-only infrastructure (no physical servers). Google data centers: ISO 27001, SOC 2, PCI DSS certified.	
164.310(a)(2)(i)	Contingency Operations	Addressable	✅ Implemented	Multi-region deployment ensures continuity even with data center failure.

Standard	Implementation Specification	Status	IHEP Implementation	
164.310(a)(2)(ii)	Facility Security Plan	Addressable	✅ Implemented	Rely on Google Cloud's facility security (24/7 guards, biometric access, video surveillance).
164.310(a)(2)(iii)	Access Control and Validation Procedures	Addressable	✅ Implemented	Office access: badge readers (HID). Visitor log. Escorts required.
164.310(a)(2)(iv)	Maintenance Records	Addressable	✅ Implemented	Google Cloud maintains infrastructure logs. Equipment maintenance tracked in ServiceNow.
164.310(b) Workstation Use	Required	✅ Implemented	Acceptable use policy (AUP). Endpoint protection. Auto-lock after 5 minutes idle.	
164.310(c) Workstation Security	Required	✅ Implemented	Full disk encryption (FileVault/BitLocker). Device management (Jamf/Intune). Remote wipe capability.	
164.310(d)(1) Device and Media Controls	Required	✅ Implemented	Media disposal policy: physical destruction or DoD 5220.22-M wipe. Certificate of destruction retained.	
164.310(d)(2)(i)	Disposal	Required	✅ Implemented	Hard drives shredded (Iron Mountain). Cloud data: crypto-shredding (delete encryption keys).
164.310(d)(2)(ii)	Media Re-use	Required	✅ Implemented	Devices sanitized per NIST SP 800-88 before re-use or donation.
164.310(d)(2)(iii)	Accountability	Addressable	✅ Implemented	Asset inventory (Snipe-IT). Check-in/check-out procedures. Annual asset audit.
164.310(d)(2)(iv)	Data Backup and Storage	Addressable	✅ Implemented	Backups encrypted at rest. Stored in secure GCS buckets with IAM controls.

1.3 Technical Safeguards

Standard	Implementation Specification	Status	IHEP Implementation	
164.312(a)(1) Access Control	Required	✅ Implemented	Zero Trust architecture. Unique user IDs. MFA required. Session timeout: 15 minutes.	
164.312(a)(2)(i)	Unique User Identification	Required	✅ Implemented	Every user has unique UUID. Shared accounts prohibited. Service accounts use dedicated credentials.
164.312(a)(2)(ii)	Emergency Access Procedure	Required	✅ Implemented	Break-glass accounts for emergencies. Requires two-person authorization. All usage audited.
164.312(a)(2)(iii)	Automatic Logoff	Addressable	✅ Implemented	Idle timeout: 15 minutes (web), 30 minutes (mobile). JWT tokens expire after 15 minutes.
164.312(a)(2)(iv)	Encryption and Decryption	Addressable	✅ Implemented	AES-256-GCM at rest. TLS 1.3 in transit. Field-level encryption for PHI. Cloud KMS key management.
164.312(b) Audit Controls	Required	✅ Implemented	Comprehensive audit logging. Immutable trail (blockchain chaining). Logs exported to BigQuery (7-year retention).	
164.312(c)(1) Integrity	Required	✅ Implemented	Cryptographic hashing (SHA-256). Digital signatures for critical data. Data validation on all inputs.	
164.312(c)(2)	Mechanism to Authenticate ePHI	Addressable	✅ Implemented	HMAC for message authentication. TLS certificates for system authentication. Digital signatures for documents.
164.312(d) Person or Entity Authentication	Required	✅ Implemented	Multi-factor authentication (MFA). Biometric option (mobile). Certificate-based auth for services.	
164.312(e)(1) Transmission Security	Required	✅ Implemented	TLS 1.3 for all external communications. VPN for remote access. Encrypted email (S/MIME).	

Standard	Implementation Specification	Status	IHEP Implementation	
164.312(e)(2)(i)	Integrity Controls	Addressable	✅ Implemented	Message digests (SHA-256). Sequence numbers prevent replay attacks.
164.312(e)(2)(ii)	Encryption	Addressable	✅ Implemented	All data in transit encrypted (TLS 1.3). Perfect forward secrecy enabled.

2. NIST SP 800-53r5 Control Mapping

2.1 Control Family: Access Control (AC)

Control	Control Name	Implementation Status	Technical Implementation
AC-1	Policy and Procedures	✅ Fully Implemented	Access control policy documented (v2.3, reviewed annually). Procedures in runbooks.
AC-2	Account Management	✅ Fully Implemented	Automated provisioning (Cloud Identity). Quarterly access reviews. Immediate de-provisioning on termination.
AC-2(1)	Automated System Account Management	✅ Fully Implemented	Terraform provisions service accounts. GitHub Actions automates IAM role assignments.
AC-2(2)	Automated Temporary Account Management	✅ Fully Implemented	Temporary access auto-expires after 8 hours. Logged in audit trail.
AC-2(3)	Disable Accounts	✅ Fully Implemented	Inactive accounts disabled after 90 days. Script runs weekly to check last login timestamp.
AC-2(4)	Automated Audit Actions	✅ Fully Implemented	All account actions logged to Cloud Logging → BigQuery. Alerts on suspicious activity.
AC-3	Access Enforcement	✅ Fully Implemented	Role-Based Access Control (RBAC) enforced by IAM service. Zero Trust validates every request.
AC-4	Information Flow Enforcement	✅ Fully Implemented	Network segmentation via VPC. Firewall rules enforce allowed traffic flows. VPC Service Controls prevent data exfiltration.
AC-5	Separation of Duties	✅ Fully Implemented	No single person can deploy to production. Code requires peer review. Deployments require approval from different person.
AC-6	Least Privilege	✅ Fully Implemented	Default deny. Users granted minimum necessary permissions. Privilege escalation requires justification + approval.
AC-6(1)	Authorize Access to Security Functions	✅ Fully Implemented	Security admin role separate from regular admin. Multi-person approval for security changes.
AC-6(2)	Non-Privileged Access for Nonsecurity Functions	✅ Fully Implemented	Standard accounts have no admin rights. Elevated access via temporary privilege escalation.

Control	Control Name	Implementation Status	Technical Implementation
AC-7	Unsuccessful Logon Attempts	✅ Fully Implemented	5 failed attempts = 15-minute lockout. 10 attempts = 1-hour lockout. Alerts sent to security team.
AC-8	System Use Notification	✅ Fully Implemented	Banner displayed on login: "Authorized use only. Activity monitored and logged." Requires acceptance.
AC-11	Device Lock	✅ Fully Implemented	Auto-lock after 5 minutes idle (workstations). 2 minutes for mobile devices. Requires re-authentication.
AC-12	Session Termination	✅ Fully Implemented	Sessions terminate after 15 minutes idle. JWT tokens expire (cannot be extended).
AC-14	Permitted Actions Without Identification	✅ Fully Implemented	Public pages (marketing site) accessible. All healthcare functions require authentication.
AC-17	Remote Access	✅ Fully Implemented	VPN required for internal systems (ZScaler). MFA mandatory. Remote sessions encrypted.
AC-17(1)	Monitoring and Control	✅ Fully Implemented	VPN connections logged. Anomalous locations flagged. Geographic restrictions configurable.
AC-18	Wireless Access	✅ Fully Implemented	Office Wi-Fi: WPA3-Enterprise. Guest network isolated. Mobile apps use TLS.
AC-19	Access Control for Mobile Devices	✅ Fully Implemented	MDM enrolled (Jamf/Intune). Encryption required. Remote wipe enabled. Jailbroken devices blocked.
AC-20	Use of External Systems	✅ Fully Implemented	BYOD prohibited for PHI access. Contractor devices must meet security baseline.

2.2 Control Family: Audit and Accountability (AU)

Control	Control Name	Implementation Status	Technical Implementation
AU-1	Policy and Procedures	✅ Fully Implemented	Audit policy v1.8 (annual review). Logging standards documented.
AU-2	Event Logging	✅ Fully Implemented	All security-relevant events logged: authentication, PHI access, admin actions, system errors.
AU-2(3)	Reviews and Updates	✅ Fully Implemented	Logged events reviewed quarterly. Policy updated based on incident learnings.
AU-3	Content of Audit Records	✅ Fully Implemented	Logs contain: timestamp, user ID, action, resource, result, IP, trust score.
AU-4	Audit Log Storage Capacity	✅ Fully Implemented	BigQuery scales automatically. Current retention: 7 years. Monitoring alerts if approaching limits.
AU-5	Response to Audit Logging Process Failures	✅ Fully Implemented	If logging fails, system enters read-only mode. Alerts sent to on-call.
AU-6	Audit Record Review, Analysis, and Reporting	✅ Fully Implemented	Daily automated analysis (anomaly detection). Weekly human review. Monthly executive report.

Control	Control Name	Implementation Status	Technical Implementation
AU-6(1)	Automated Process Integration	✅ Fully Implemented	Security Information and Event Management (SIEM) aggregates logs. ML detects anomalies.
AU-6(3)	Correlate Audit Record Repositories	✅ Fully Implemented	Logs from all services centralized in BigQuery. Correlation queries identify attack patterns.
AU-7	Audit Record Reduction and Report Generation	✅ Fully Implemented	Looker dashboards visualize key metrics. Custom reports generated on-demand (SQL queries).
AU-8	Time Stamps	✅ Fully Implemented	All logs use UTC timestamps (ISO 8601 format). NTP sync with Google's time servers.
AU-9	Protection of Audit Information	✅ Fully Implemented	Audit logs append-only (no delete permissions). Blockchain chaining detects tampering.
AU-9(2)	Store on Separate Physical Systems	✅ Fully Implemented	Logs exported from application servers to BigQuery (separate infrastructure).
AU-10	Non-Repudiation	✅ Fully Implemented	Digital signatures on critical transactions. Immutable audit trail prevents denial of actions.
AU-11	Audit Record Retention	✅ Fully Implemented	7-year retention (HIPAA requirement). Archived logs in Cloud Storage Nearline.
AU-12	Audit Record Generation	✅ Fully Implemented	Logging libraries in all services. Centralized configuration (enable/disable audit events).

2.3 Control Family: Configuration Management (CM)

Control	Control Name	Implementation Status	Technical Implementation
CM-1	Policy and Procedures	✅ Fully Implemented	Configuration management plan v1.4. Change control board meets weekly.
CM-2	Baseline Configuration	✅ Fully Implemented	Infrastructure as Code (Terraform). Container images versioned in Artifact Registry.
CM-2(2)	Automation Support for Accuracy/Currency	✅ Fully Implemented	Terraform state managed in GCS. Drift detection runs daily.
CM-3	Configuration Change Control	✅ Fully Implemented	All changes via pull requests. Peer review required. Automated testing before merge.
CM-3(2)	Testing, Validation, and Documentation	✅ Fully Implemented	Staging environment mirrors production. Changes tested in staging. Rollback plan documented.
CM-4	Impact Analyses	✅ Fully Implemented	Change impact assessment required for production changes. Security review for high-risk changes.
CM-5	Access Restrictions for Change	✅ Fully Implemented	Production deployments require approval. Only release engineers can deploy.
CM-6	Configuration Settings	✅ Fully Implemented	Security baselines defined (CIS benchmarks). Configuration templates in Terraform.

Control	Control Name	Implementation Status	Technical Implementation
CM-7	Least Functionality	✅ Fully Implemented	Containers include only necessary packages. Unused services disabled. Minimal OS attack surface.
CM-8	System Component Inventory	✅ Fully Implemented	Asset inventory in Snipe-IT. Cloud resources tracked via Terraform. Weekly inventory reconciliation.
CM-9	Configuration Management Plan	✅ Fully Implemented	CM plan documents roles, processes, tools. Updated quarterly.
CM-10	Software Usage Restrictions	✅ Fully Implemented	Only approved software installed (whitelist). License compliance tracked.
CM-11	User-Installed Software	✅ Fully Implemented	Standard users cannot install software. Admin approval required via ServiceNow.

2.4 Control Family: Identification and Authentication (IA)

Control	Control Name	Implementation Status	Technical Implementation
IA-1	Policy and Procedures	✅ Fully Implemented	Identity management policy v2.1. Procedures documented in wiki.
IA-2	Identification and Authentication	✅ Fully Implemented	All users uniquely identified. Authentication required for all functions accessing PHI.
IA-2(1)	Multi-Factor Authentication	✅ Fully Implemented	MFA mandatory for all users. TOTP (Google Authenticator), SMS, or biometric.
IA-2(2)	Multi-Factor Authentication to Privileged Accounts	✅ Fully Implemented	Admin accounts require MFA. Hardware tokens (YubiKey) for highest privilege.
IA-2(3)	Local Access to Privileged Accounts	N/A	Cloud-only infrastructure. No local administrative access.
IA-2(12)	Acceptance of PIV Credentials	⚠ Planned	Phase II: Support for PIV/CAC cards for federal partnerships.
IA-3	Device Identification and Authentication	✅ Fully Implemented	Devices registered in MDM. Certificate-based authentication for services.
IA-4	Identifier Management	✅ Fully Implemented	User IDs assigned upon hire. Never reused. Disabled IDs clearly marked.
IA-5	Authenticator Management	✅ Fully Implemented	Passwords: 12+ chars, complexity, no reuse. Stored as bcrypt hashes (cost 14).
IA-5(1)	Password-Based Authentication	✅ Fully Implemented	Password policy enforced. Compromised password detection (Have I Been Pwned API).
IA-5(2)	PKI-Based Authentication	✅ Fully Implemented	Service-to-service auth uses mutual TLS. Certificate rotation automated.
IA-6	Authentication Feedback	✅ Fully Implemented	Password fields masked. Failed login messages generic ("Invalid credentials").

Control	Control Name	Implementation Status	Technical Implementation
IA-7	Cryptographic Module Authentication	✅ Fully Implemented	Cloud KMS is FIPS 140-2 Level 3 validated.
IA-8	Identification and Authentication (Non-Org Users)	✅ Fully Implemented	External collaborators use federated identity (Google Workspace, Azure AD).

2.5 Control Family: System and Communications Protection (SC)

Control	Control Name	Implementation Status	Technical Implementation
SC-1	Policy and Procedures	✅ Fully Implemented	System protection policy v1.9. Network security standards documented.
SC-2	Separation of System and User Functionality	✅ Fully Implemented	Admin interfaces separate from user interfaces. Management plane isolated.
SC-5	Denial-of-Service Protection	✅ Fully Implemented	Cloud Armor (WAF) with rate limiting. Auto-scaling absorbs traffic spikes. DDoS mitigation.
SC-7	Boundary Protection	✅ Fully Implemented	VPC firewall rules enforce perimeter. VPC Service Controls prevent data exfiltration.
SC-7(3)	Access Points	✅ Fully Implemented	All external access through API Gateway. Managed interfaces only.
SC-7(4)	External Telecommunications Services	✅ Fully Implemented	VPN for remote access. Encrypted tunnels for partner integrations.
SC-7(5)	Deny by Default / Allow by Exception	✅ Fully Implemented	Firewall default policy: DENY. Explicit allow rules required.
SC-8	Transmission Confidentiality and Integrity	✅ Fully Implemented	TLS 1.3 for all external communications. IPSec for VPN. Perfect forward secrecy.
SC-8(1)	Cryptographic Protection	✅ Fully Implemented	All transmitted PHI encrypted. Strong cipher suites only (TLS_AES_256_GCM_SHA384).
SC-12	Cryptographic Key Establishment and Management	✅ Fully Implemented	Cloud KMS manages keys. 90-day rotation. Keys never exported.
SC-13	Cryptographic Protection	✅ Fully Implemented	FIPS 140-2 validated algorithms. AES-256-GCM, RSA-4096, SHA-256.
SC-17	Public Key Infrastructure Certificates	✅ Fully Implemented	Let's Encrypt certificates (auto-renew). Internal CA for service mesh.
SC-20	Secure Name/Address Resolution Service	✅ Fully Implemented	Cloud DNS with DNSSEC. Split-horizon DNS (internal vs external).
SC-23	Session Authenticity	✅ Fully Implemented	JWT tokens signed with RS256. Tokens include user ID, expiry, trust score.
SC-28	Protection of Information at Rest	✅ Fully Implemented	All data encrypted at rest. AES-256-GCM. Keys in Cloud KMS.

2.6 Control Family: System and Information Integrity (SI)

Control	Control Name	Implementation Status	Technical Implementation
SI-1	Policy and Procedures	✅ Fully Implemented	System integrity policy v1.6. Malware protection plan documented.
SI-2	Flaw Remediation	✅ Fully Implemented	Vulnerability scanning (Qualys). Critical patches within 24 hours. Patch tracking in Jira.
SI-2(2)	Automated Flaw Remediation Status	✅ Fully Implemented	Dependabot creates PRs for dependency updates. Snyk scans containers.
SI-3	Malicious Code Protection	✅ Fully Implemented	Endpoint protection (CrowdStrike). Email filtering (Proofpoint). Web gateway (Zscaler).
SI-3(1)	Central Management	✅ Fully Implemented	CrowdStrike Falcon console centrally manages endpoints. Policies pushed from console.
SI-4	System Monitoring	✅ Fully Implemented	Cloud Monitoring for infrastructure. Application Performance Monitoring (APM). Security alerts.
SI-4(2)	Automated Tools for Real-Time Analysis	✅ Fully Implemented	SIEM (Chronicle) analyzes logs in real-time. ML anomaly detection. Automated alerts.
SI-4(5)	System-Generated Alerts	✅ Fully Implemented	Alerts sent to PagerDuty (critical) or email (warning). On-call rotation for response.
SI-5	Security Alerts, Advisories, and Directives	✅ Fully Implemented	Subscribe to US-CERT, vendor bulletins. Security team reviews daily. Action items created.
SI-7	Software, Firmware, and Information Integrity	✅ Fully Implemented	Container image signing (cosign). Git commits signed (GPG). Checksums verified.
SI-7(1)	Integrity Checks	✅ Fully Implemented	File integrity monitoring (FIM) on critical configs. Alerts on unauthorized changes.
SI-8	Spam Protection	✅ Fully Implemented	Proofpoint blocks spam (>99% accuracy). User reporting button for misclassified emails.
SI-10	Information Input Validation	✅ Fully Implemented	All API inputs validated against OpenAPI schemas. SQL injection prevention (parameterized queries).
SI-11	Error Handling	✅ Fully Implemented	Generic error messages to users. Detailed errors logged internally. No stack traces exposed.
SI-12	Information Management and Retention	✅ Fully Implemented	Data retention policy: PHI 6 years post-last-treatment. Logs 7 years. Automated purge.

3. Compliance Roadmap

3.1 Current State (November 2025)

Achieved:

- ✅ HIPAA Security Rule: 100% compliance
- ✅ NIST SP 800-53r5: 164/179 controls (91.6%)
- ✅ SOC 2 Type I: Audit completed September 2025 (no findings)

In Progress:

- 🔄 HITRUST CSF i1 Certification (expected Q1 2026)
- 🔄 SOC 2 Type II (12-month observation period, completion Q2 2026)

3.2 Phase I Compliance Targets (Months 1-12)

Milestone	Target Date	Status
HIPAA Compliance Program Established	Month 1	✅ Complete
Third-Party Security Assessment	Month 6	✅ Complete
HITRUST i1 Application Submitted	Month 9	✅ Complete
SOC 2 Type I Audit	Month 9	✅ Complete
Penetration Test (External)	Month 12	🔄 Scheduled

3.3 Phase II Compliance Targets (Months 13-24)

Milestone	Target Date	Status
HITRUST i1 Certification Achieved	Month 15 (Q1 2026)	🔄 In Progress
SOC 2 Type II Audit Complete	Month 18 (Q2 2026)	🔄 In Progress
FedRAMP Moderate Readiness Assessment	Month 24 (Q4 2026)	📋 Planned
GDPR Compliance (EU Expansion)	Month 24	📋 Planned

3.4 Phase III Compliance Targets (Months 25-36)

Milestone	Target Date	Status
HITRUST r2 Certification	Month 30 (Q2 2027)	📋 Planned
FedRAMP Moderate Authorization	Month 36 (Q4 2027)	📋 Planned
ISO 27001 Certification	Month 36	📋 Planned

4. Business Associate Agreement (BAA) Management

4.1 BAA Inventory

IHEP maintains Business Associate Agreements with all vendors handling PHI:

Vendor	Service	BAA Status	Last Review
Google Cloud Platform	Infrastructure & PHI Storage	✅ Executed	Nov 2025
Twilio	SMS Notifications	✅ Executed	Oct 2025
SendGrid	Email Notifications	✅ Executed	Oct 2025
Mixpanel	Analytics (de-identified only)	N/A	No PHI
Sentry	Error Tracking (scrubbed logs)	N/A	No PHI

BAA Review Process:

1. Legal review of vendor BAA template
2. Negotiation of terms (30-day breach notification, encryption requirements)
3. Executive signature (CEO or COO)
4. Annual renewal review
5. Vendor security questionnaires (SIG Lite)

4.2 Subcontractor Management

All subcontractors (Business Associates of Business Associates) must:

- Execute BAA with IHEP or prime vendor
- Undergo security assessment (questionnaire minimum)
- Meet IHEP security baseline requirements
- Submit to annual audits

5. Security Incident Response

5.1 Incident Classification

Severity	Definition	Response Time	Notification
Critical	PHI breach, ransomware, system compromise	<15 minutes	CEO, CISO, Legal
High	Unauthorized access attempt, malware detection, DDoS	<1 hour	CISO, Security Team
Medium	Failed security controls, policy violations	<4 hours	Security Team
Low	Security warnings, suspicious activity	<24 hours	Security Analyst

5.2 Incident Response Procedures

1. Detection & Analysis (15 minutes)

- Alert triggers PagerDuty notification
- On-call security analyst reviews alert
- Determine severity and classify incident
- Initiate incident response war room (Zoom)

2. Containment (30 minutes)

- Isolate affected systems (firewall rules, disable accounts)
- Preserve evidence (snapshot VMs, export logs)
- Prevent lateral movement

3. Eradication (varies)

- Remove malware, close vulnerabilities
- Reset compromised credentials
- Patch systems

4. Recovery (varies)

- Restore from clean backups
- Verify system integrity
- Gradual return to normal operations

5. Post-Incident Review (within 72 hours)

- Root cause analysis
- Lessons learned documentation
- Update runbooks and controls
- Communicate to stakeholders

5.3 Breach Notification

Per HIPAA 164.404, if PHI breach affects >500 individuals:

- **HHS Notification:** Within 60 days
- **Media Notification:** Prominent media outlets (if >500 in state/jurisdiction)
- **Individual Notification:** Written notice within 60 days

Breach Documentation:

- Date of discovery
- Number of individuals affected
- Type of PHI involved

- Mitigation actions taken
- Notification dates

6. Third-Party Security Assessments

6.1 Completed Assessments

SOC 2 Type I (September 2025)

- **Auditor:** Deloitte & Touche LLP
- **Opinion:** Unqualified (no exceptions)
- **Scope:** Security, Availability, Confidentiality
- **Key Findings:** All controls operating effectively

Penetration Test (October 2025)

- **Firm:** Bishop Fox
- **Scope:** External network, web applications, APIs
- **Findings:** 2 medium-risk issues (remediated), 0 critical/high
- **Re-test:** All issues verified fixed

HIPAA Security Assessment (August 2025)

- **Firm:** Clearwater Compliance
- **Scope:** Administrative, Physical, Technical Safeguards
- **Findings:** 100% compliant, 3 recommendations (implemented)

6.2 Ongoing Assessments

Vulnerability Scanning (Weekly)

- **Tool:** Qualys
- **Scope:** All internet-facing assets
- **SLA:** Critical vulnerabilities patched within 24 hours

Dependency Scanning (Continuous)

- **Tools:** Snyk (containers), Dependabot (code)
- **Action:** Automated PRs for updates

Code Security Analysis (Every Commit)

- **Tools:** SonarQube, Bandit (Python), gosec (Go)
- **Gate:** Pull requests blocked if critical issues detected

7. Employee Security Training

7.1 Training Requirements

Training	Frequency	Completion Rate	Method
HIPAA Awareness	Annual	100% (required)	Online (KnowBe4)
Security Awareness	Annual	100% (required)	Online + Quiz
Phishing Simulations	Monthly	95% click rate <5%	KnowBe4
Role-Specific Security	Onboarding + Annual	100%	In-person + Online
Incident Response	Quarterly (security team)	100%	Tabletop Exercise

7.2 Security Champions Program

- **Purpose:** Embed security in each team
- **Selection:** Volunteers from engineering, product, operations
- **Training:** Monthly security deep dives (1 hour)
- **Responsibilities:**
  - Conduct security design reviews
  - Promote secure coding practices
  - Escalate security concerns
- **Recognition:** Certificate, bonus consideration, conference attendance

8. Continuous Compliance Monitoring

8.1 Automated Compliance Checks

```
# Daily compliance checks (automated script)
compliance_checks = {
    "hipaa_audit_logging": {
        "check": "All PHI access events logged in last 24 hours",
        "query": "SELECT COUNT(*) FROM audit_logs WHERE action='PHI_ACCESS' AND timestamp
        "expected": "&gt; 0"
    },
    "encryption_at_rest": {
        "check": "All databases encrypted",
        "command": "gcloud sql instances list --format='table(name,settings.encryption)'
        "expected": "0 results"
    },
    "mfa_enabled": {
        "check": "All users have MFA enabled",
        "query": "SELECT COUNT(*) FROM users WHERE mfa_enabled = FALSE AND account_status
        "expected": "0"
    },
    "backup_completion": {
```

```
        "check": "All backups completed successfully in last 24 hours",
        "api": "cloud_sql_admin.list_backup_runs()",
        "expected": "all_status = SUCCESS"
    }
}
```

Alert on Failures: Send to #security-alerts Slack channel + PagerDuty for critical failures

8.2 Quarterly Compliance Review

Attendees: CEO, CISO, Legal Counsel, Compliance Officer, Audit Committee (investors)

Agenda:

1. Compliance dashboard review (KPIs)
2. Recent audit findings and remediation status
3. Regulatory changes and impact analysis
4. Risk register review (top 10 risks)
5. Upcoming certification milestones
6. Budget and resource needs

Deliverable: Compliance scorecard to board of directors

9. Risk Management

9.1 Risk Assessment Methodology (NIST SP 800-30)

Annual Risk Assessment Process:

1. **System Characterization**
   - Identify all systems processing PHI
   - Document data flows
   - Map system interconnections
2. **Threat Identification**
   - Internal threats (malicious insider, negligent employee)
   - External threats (hacker, ransomware, DDoS)
   - Environmental (power outage, natural disaster)
3. **Vulnerability Identification**
   - Technical vulnerabilities (scan results)
   - Procedural vulnerabilities (policy gaps)
   - Organizational vulnerabilities (insufficient staffing)
4. **Likelihood Determination**

- High: Expected to occur within 1 year
- Medium: Expected every 1-3 years
- Low: Expected > 3 years

5. **Impact Analysis**
   - Categorize impact: Low (< $100K), Medium ($100K-$1M), High (> $1M or PHI breach)
   - Consider: Financial loss, reputational damage, regulatory penalties, operational disruption
6. **Risk Calculation**
   - Risk Level = Likelihood × Impact
   - Prioritize High and Medium risks for treatment
7. **Risk Treatment**
   - Mitigate (implement controls)
   - Transfer (insurance)
   - Accept (document decision)
   - Avoid (discontinue risky activity)

9.2 Current Risk Register (Top 10)

ID	Risk	Likelihood	Impact	Risk Score	Mitigation
R-01	PHI data breach due to insider threat	Medium	High	15	Background checks, least privilege, audit logging, DLP
R-02	Ransomware attack	Medium	High	15	Endpoint protection, backups, email filtering, training
R-03	Healthcare API rate limit exceeded	High	Medium	12	Request caching, quota monitoring, fallback procedures
R-04	Third-party vendor breach (BAA)	Medium	High	12	Vendor assessments, BAA terms, insurance requirements
R-05	Key personnel departure (CISO, CTO)	Medium	Medium	9	Succession planning, cross-training, retention bonuses
R-06	DDoS attack causing service outage	Medium	Medium	9	Cloud Armor, auto-scaling, CDN, incident response plan
R-07	AI model bias causing harm to patients	Low	High	9	Bias testing, human-in-loop, ethics board, explainability
R-08	Compliance audit failure (HITRUST)	Low	High	9	Mock audits, gap assessments, compliance automation
R-09	Database performance degradation	High	Low	6	Connection pooling, read replicas, query optimization
R-10	Natural disaster affecting GCP region	Low	Medium	6	Multi-region architecture, disaster recovery plan, tests

10. Insurance Coverage

10.1 Cyber Insurance Policy

Carrier: Coalition (cyber insurance specialist)
Policy Number: CYB-2025-IHEP-001
Coverage Period: Jan 1, 2025 - Dec 31, 2025
Premium: $48,000/year

Coverage Limits:

- **Cyber Liability:** $10M per occurrence, $10M aggregate
- **Data Breach Response:** $5M (forensics, notification, credit monitoring)
- **Business Interruption:** $2M (lost revenue during outage)
- **Ransomware/Extortion:** $1M (payment + negotiation)
- **Regulatory Defense:** $5M (HIPAA investigations, fines)

Deductible: $25,000 per claim

Requirements:

- MFA enabled for all users
- Endpoint protection deployed
- Backups tested quarterly
- Annual penetration test
- Security awareness training

Conclusion

IHEP's security and compliance program demonstrates institutional commitment to protecting patient privacy and maintaining regulatory compliance. Key achievements:

- **164 NIST SP 800-53r5 controls fully implemented** (91.6% coverage)
- **100% HIPAA Security Rule compliance** across all safeguards
- **Zero security incidents** since inception
- **SOC 2 Type I certified** with no findings
- **HITRUST i1 certification in progress** (expected Q1 2026)

Our security-first architecture, combined with rigorous compliance monitoring and third-party validation, provides investors and partners confidence that IHEP meets the highest standards for healthcare data protection.

Document Control
Classification: Security & Compliance - Confidential
Version: 1.1

Last Updated: November 26, 2025
Next Review: January 2026