CONFIDENTIAL | PROPRIETARY | RESTRICTED

Cognera Health

Compliance Governance Framework

NOTICE OF CONFIDENTIALITY

This document contains confidential, proprietary, trade secret, security-sensitive, compliance-sensitive, privacy-sensitive, operationally sensitive, and commercially valuable information belonging to Cognera Health, Inc.

This document is provided solely for authorized business, compliance, security, privacy, governance, procurement, audit, due diligence, regulatory, partnership, customer evaluation, investment, or contractual purposes.

Unauthorized access, review, copying, reproduction, extraction, modification, distribution, publication, disclosure, transfer, transmission, storage, sharing, screenshotting, photographing, summarization, recording, indexing, scraping, training of artificial intelligence systems, machine learning systems, large language models, data mining systems, or other use is strictly prohibited without the prior written consent of Cognera Health.

This document and its contents constitute proprietary and confidential information and may include trade secrets protected by applicable intellectual property, trade secret, privacy, cybersecurity, healthcare, and commercial laws.

Possession of this document does not grant any ownership rights, intellectual property rights, license rights, reproduction rights, derivative work rights, publication rights, disclosure rights, training rights, or distribution rights.

Any unauthorized use may result in:

- Immediate revocation of access
- Contractual remedies
- Injunctive relief
- Civil liability
- Regulatory action
- Criminal penalties where applicable
- Recovery of damages
- Recovery of attorneys' fees and costs

By accessing, reviewing, receiving, downloading, storing, or using this document, the recipient acknowledges and agrees to comply with these restrictions.

Document Version Table

Version	Date	Author	Description
Draft 1.0	03/15/2025	John Budala	Initial draft created.
Draft 1.1	01/06/2026	John Budala	Added AI governance, authorization expansion, voice-to-text security, and AI risk management

Table of Contents

1. Introduction

Cognera Health is a healthcare technology company that provides Software-as-a-Service (SaaS) solutions, including HealScript™, HealConnect™ and related platforms designed to support mental health, behavioral health, wellness, integrated care, care coordination, clinical operations, and continuous care delivery.

As a Business Associate (BA) under the Health Insurance Portability and Accountability Act (HIPAA), Cognera Health processes, stores, transmits, and protects Protected Health Information (PHI), electronic Protected Health Information (ePHI), personal information, consumer health data, and other sensitive information on behalf of healthcare providers, organizations, and authorized customers.

This Compliance Governance Framework establishes the governance structures, policies, procedures, controls, and oversight mechanisms necessary to support privacy, security, compliance, risk management, artificial intelligence governance, information governance, operational resilience, and continuous improvement across all Cognera Health products, services, personnel, systems, and operations.

The framework is designed to support regulatory compliance, industry best practices, customer obligations, contractual requirements, and enterprise governance expectations while maintaining the confidentiality, integrity, availability, privacy, security, and responsible use of information entrusted to Cognera Health.

Through a risk-based and compliance-driven approach, Cognera Health is committed to protecting sensitive information, supporting healthcare organizations, maintaining regulatory readiness, and fostering trust among clients, providers, individuals, partners, regulators, and stakeholders.

1.1 Scope and Applicability

This Compliance Governance Framework applies to all Cognera Health cloud-based platforms, applications, services, integrations, infrastructure, personnel, operations, business processes, third-party providers, and supporting technologies.
The framework governs the collection, creation, processing, storage, transmission, access, use, disclosure, retention, deletion, destruction, and protection of:

- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)
- Personal Information (PI)
- Personal Data

- Sensitive Personal Information
- Consumer Health Data
- Clinical Documentation
- Behavioral Health Information
- Wellness Data
- Artificial Intelligence (AI) Processing Data
- Operational Data
- Security Records
- Audit Records
- Customer Information
- Vendor Information
- Other confidential and regulated information processed by Cognera Health

This framework applies to:

- Employees
- Contractors
- Consultants
- Temporary Personnel
- Interns
- Volunteers
- Third-Party Vendors
- Business Associates
- Subcontractors
- Cloud Service Providers (CSPs)
- Managed Service Providers (MSPs)
- Managed Security Service Providers (MSSPs)
- All authorized users of Cognera Health systems and services

Where Cognera Health utilizes secure cloud infrastructure providers, certain physical safeguards may be implemented through contracted cloud service providers and associated shared-responsibility models. Cognera Health maintains oversight and governance responsibilities for applicable privacy, security, compliance, and operational controls regardless of deployment architecture.

1.2 Regulatory and Standards Alignment

Policy: Cognera Health maintains its privacy, security, compliance, risk management, information governance, artificial intelligence governance, and operational control programs in alignment with

applicable healthcare regulations, privacy laws, cybersecurity standards, industry-recognized frameworks, and emerging best practices.

This Compliance Governance Framework establishes the foundational governance structure supporting compliance obligations, risk management activities, security controls, privacy protections, operational safeguards, and responsible technology practices across the organization.

While HIPAA and HITECH serve as primary healthcare regulatory foundations, Cognera Health recognizes that modern healthcare technology platforms operate within a broader regulatory, security, privacy, and governance landscape. Accordingly, Cognera Health incorporates controls, principles, and governance practices that support alignment with additional privacy, security, compliance, and operational frameworks where applicable.

United States Healthcare and Privacy Regulations

Cognera Health's compliance program is designed to support applicable requirements arising from:

- Health Insurance Portability and Accountability Act (HIPAA)
- HIPAA Privacy Rule (45 CFR Part 160 and Part 164)
- HIPAA Security Rule (45 CFR §164.302–318)
- HIPAA Breach Notification Rule (45 CFR §164.400–414)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Federal Trade Commission (FTC) requirements
- Applicable state healthcare privacy laws
- Applicable state breach notification laws
- Applicable state consumer privacy regulations
- Applicable telehealth and behavioral health regulatory requirements

International Privacy and Data Protection Frameworks

Where applicable to customers, users, contractual obligations, or operational activities, Cognera Health incorporates governance principles and controls informed by:

- General Data Protection Regulation (GDPR)
- UK General Data Protection Regulation (UK GDPR)
- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Other applicable privacy regulations and data protection requirements

Cognera Health supports privacy principles including:

- Lawfulness, fairness, and transparency

- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability
- Individual privacy rights
- Responsible data stewardship

Security and Compliance Frameworks

Cognera Health's security and compliance controls are informed by recognized industry frameworks including:

- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001 Information Security Management Systems (ISMS)
- ISO/IEC 27701 Privacy Information Management Systems (PIMS)
- SOC 2 Trust Services Criteria
- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 Security and Privacy Controls
- NIST SP 800-66 HIPAA Security Rule Guidance
- NIST SP 800-88 Media Sanitization Guidelines
- Center for Internet Security (CIS) Controls

These frameworks support the implementation of administrative, technical, operational, and organizational safeguards designed to protect information assets and reduce organizational risk.

Artificial Intelligence Governance

Cognera Health applies responsible artificial intelligence governance principles to the design, development, deployment, operation, monitoring, and oversight of AI-enabled capabilities.

AI governance practices emphasize:

- Human-in-the-loop oversight
- Transparency
- Explainability
- Accountability
- Privacy protection
- Security

- Risk management
- Clinical oversight
- Bias monitoring
- Model governance
- Auditability
- Responsible innovation
- Continuous monitoring and validation

AI governance practices are informed by:

- NIST AI Risk Management Framework (AI RMF)
- Healthcare regulatory expectations
- Responsible AI principles
- Emerging industry standards
- Clinical best practices
- Organizational risk management requirements

AI systems deployed by Cognera Health are intended to support, augment, and enhance clinical, operational, and decision-support activities and shall not independently diagnose, prescribe, treat, or make final clinical determinations without appropriate human oversight and review.

Applicability

Compliance obligations applicable to specific customers, jurisdictions, contracts, services, regulatory requirements, or operational environments shall be incorporated into appropriate policies, procedures, technical controls, operational safeguards, risk management activities, contractual obligations, and governance processes.

Cognera Health continuously evaluates evolving regulatory requirements, industry standards, cybersecurity threats, privacy expectations, and emerging technologies to maintain an effective, scalable, and risk-based compliance governance program that supports organizational growth, customer trust, operational excellence, and regulatory readiness.

1.3 Related Governance Documents

This Compliance Governance Framework serves as the primary governance document for privacy, security, compliance, risk management, artificial intelligence governance, workforce training, incident response, business associate management, and operational safeguards implemented by Cognera Health.

Certain specialized compliance domains may be governed by separate supporting documents where additional operational detail, procedures, controls, retention schedules, or regulatory requirements are necessary.

At the time of publication, the following related governance document is maintained:

• Data Retention, Deletion, and Secure Disposal Policy

Additional governance documents may be developed as the Cognera Health compliance program matures.

Where conflicts exist between this Compliance Governance Framework and any related governance document, the Compliance Governance Framework shall serve as the governing authority unless otherwise required by law or regulation.

2. Governance Structure

2.1 Compliance Officer

- **Role**: Oversees HIPAA compliance across all operations and solutions.
- **Reporting**: Reports to the Chief Information Security Officer (CISO).
- **Responsibilities**:
  - Develop and update HIPAA-compliant policies.
  - Conduct annual risk assessments and oversee third-party audits.
  - Serve as the primary contact for HIPAA inquiries and incidents.
  - Collaborate with Cloud Service Providers (CSPs), Managed Service Providers (MSPs), and Managed Security Service Providers (MSSPs) for security monitoring.
  - Designate a backup Compliance Officer for continuity.
  - Maintain an inventory of PHI-containing systems.
  - Report compliance status monthly to leadership.
- **Qualifications**: Certified in Healthcare Privacy Compliance (CHPC) or equivalent, with five years of experience in HIPAA, healthcare IT, and SaaS.
- **Delegation**: In absence, the backup officer assumes duties with notification to the CISO and Steering Committee.

2.2 Steering Committee

- **Composition**: Senior leaders from IT, Legal, HR, Operations, and Product Development.
- **Responsibilities**:
  - Approve HIPAA policies annually or after regulatory changes.
  - Oversee breach response per the HIPAA Breach Notification Rule (45 CFR § 164.400-414).
  - Evaluate security controls, privacy practices, and training effectiveness.
  - Allocate resources for compliance initiatives.
  - **Meetings**: Quarterly, with ad-hoc sessions for breaches or critical updates.

2.3 Business Associate and Subcontractor Management

- **Policy**: Implement policies and procedures to ensure that HIPAA compliance extends to Business Associates (BAs) and their subcontractors per HIPAA Security Rule (45 CFR § 164.308(b)).
- **Procedures**:
  - Vendor Due Diligence: Assess CSPs, MSPs, MSSPs, and other vendors handling PHI:
    - Pre-engagement: Require security questionnaires, HIPAA training proof, and risk scoring (Critical/High/Medium/Low) based on PHI volume, sensitivity, and incident history.
    - Ongoing: Monitor SLAs, require semi-annual compliance attestations, and reassess after incidents or scope changes.
    - Termination: Verify data return/destruction and revoke access within 30 days.
  - Subcontractor Oversight:
    - Require notification and approval before subcontractor's access PHI, verify BAA extension, and conduct annual compliance reviews. Non-compliant subcontractors face termination.
  - Audit Rights:
    - Retain rights to audit third-party systems biennially or post-breach.

3. Privacy Policies

3.1 Use, Disclosure, and Minimum Necessary Rule

- **Policy**: PHI is restricted to the minimum necessary for workforce (employees, contractors, third-party personnel, temporary staff, and volunteers) job functions (45 CFR § 164.502(b)) and may only be used/disclosed for Treatment, Payment, and Healthcare Operations (TPO) unless authorized or legally required (45 CFR § 164.512).
- **Procedures**:
  - Limit PHI access via Role-Based Access Controls (RBAC) and quarterly reviews to revoke unnecessary privileges.
  - Require signed authorizations for non-TPO uses (e.g., marketing), stored securely.
  - Encrypt PHI transmissions and log disclosures not related to TPO.
  - De-identify PHI for research per 45 CFR § 164.514 (Safe Harbor or Expert Determination).
  - Provide accounting of disclosures to individuals within 30 days upon request.
- **Enforcement**: Violations result in disciplinary actions per Section 7.1.

3.2 Authorization Management

- **Policy:** Cognera Health will obtain, manage, and maintain valid HIPAA-compliant authorizations for any uses or disclosures of PHI that are not part of Treatment, Payment, or Healthcare Operations (TPO), including—but not limited to—AI-driven analytics, secondary

data processing, voice recordings, and advanced clinical insights, in compliance with 45 CFR § 164.508.

- **Procedures:**
  - Require explicit, written authorization for:
    - AI model training using identifiable PHI
    - Advanced analytics beyond direct care delivery
    - Voice recording and audio capture involving PHI
  - Ensure authorizations clearly describe:
    - Purpose of use or disclosure
    - Data elements involved
    - Expiration date or event
    - Right to revoke authorization
  - Maintain electronic authorization records for a minimum of six (6) years.
  - Enforce revocation of authorization within five (5) business days of receipt.
  - Prohibit conditioning treatment or services on authorization unless permitted by law.
  - Audit authorization compliance quarterly

4. Security Policies

4.1 Access and Integrity Management

- **Policy**: Restrict PHI/ePHI access to authorized workforce based on job roles (45 CFR § 164.308(a)(4), § 164.312(a)) and protect ePHI from improper alteration/destruction (45 CFR § 164.312(c)).
- **Procedures**:
  - Implement RBAC with unique user IDs; revoke access within 24 hours of role changes/termination.
  - Require Multi-Factor Authentication (MFA) and automatic lockout after 10 minutes of inactivity.
  - Log access requests and audit anomalies quarterly.
  - Use checksums, digital signatures, and transaction logging to ensure data integrity.

4.2 Data Encryption and Technical Security

- **Policy**: Encrypt PHI/ePHI at rest and in transit (45 CFR § 164.312(a)(2)(iv)) and implement technical controls across systems (45 CFR § 164.312).
- **Procedures**:
  - Use AES-256 for data at rest and TLS 1.3 for transmissions (including APIs and mobile apps).
  - Conduct annually penetration tests by a third-party firm.
  - Implement secure key management with annual rotation and dual-control access.
  - Configure cloud environments with private networking and limited public endpoints.
  - Secure mobile apps with biometric/password authentication, 5-minute timeouts, and remote wipe capability.

4.3 Device and Workstation Security

- **Policy**: Secure all devices accessing PHI (45 CFR § 164.310, § 164.312).
- **Procedures**:
  - Require endpoint protection and automatic lockout after 10 minutes on all devices (company-issued and BYOD).
  - Prohibit unencrypted removable media unless approved by the Compliance Officer.
  - Use VPNs for remote access and enforce Mobile Device Management (MDM) with encryption and wipe capabilities.
  - Apply critical patches within 7 days, high-risk within 30 days.

4.4 Voice-to-Text and Audio PHI Security

- **Policy:** Cognera Health will safeguard audio recordings, voice inputs, and transcriptions containing PHI/ePHI by implementing administrative, technical, and procedural controls, in accordance with 45 CFR § 164.312 and § 164.308.
- **Procedures:**
  - Treat all audio recordings and voice inputs as ePHI from the point of capture.
  - Require explicit consent prior to initiating any voice recording involving PHI.
  - Encrypt audio data in transit (TLS 1.3) and at rest (AES-256).
  - Restrict access to audio files and transcriptions using Role-Based Access Controls (RBAC).
  - Implement automatic deletion of raw audio files after successful transcription, validation, and completion of required quality checks unless retention is legally, contractually, or clinically required.
  - Log all access, playback, transcription, and deletion events.
  - Prohibit local storage of audio PHI on end-user devices unless encrypted and approved.
  - Conduct quarterly audits of voice-to-text workflows and vendors.

5. Patient Rights Management

- **Policy**: Support Covered Entities in fulfilling patient rights under HIPAA (45 CFR § 164.524-528).
- **Procedures**:
  - Provide electronic PHI access within 30 days, with secure authentication and audit trails.
  - Process amendment requests within 10 business days, maintaining version control.
  - Track non-TPO disclosures for six years and generate accounting reports within 5 business days.
  - Honor restriction requests with flagged access controls.

6. HITECH Act Compliance

6.1 HITECH Compliance

- **Policy**: Comply with HITECH Act provisions enhancing HIPAA protections.
- **Procedures**:
  - Prohibit PHI sale/marketing without authorization; document approvals for six years.
  - Review minimum necessary standards annually and audit compliance quarterly.
  - Acknowledge direct BA liability with annual self-assessments reported to leadership.
  - Support secure EHR integrations with API standards and detailed logs.

6.2 AI Governance and Model Oversight

- **Policy:** Cognera Health will oversee the design, implementation, and operation of Artificial Intelligence (AI) and machine learning models that handle PHI/ePHI, ensuring adherence to HIPAA, HITECH, and all applicable privacy and security regulations. AI systems will serve exclusively as clinical decision-support tools and shall not independently diagnose, treat, or make determinations without human supervision.
- **Procedures:**
  - Maintain an inventory of all AI models that access or process PHI.
  - Enforce minimum necessary data usage for AI processing.
  - Require human-in-the-loop validation for all AI-generated outputs.
  - Conduct annual AI risk and bias assessments.
  - Validate model outputs for accuracy, consistency, and clinical relevance.
  - Log AI model access, data inputs, outputs, and overrides.
  - Prohibit reuse of PHI for AI model training without documented authorization.
  - Review AI governance controls annually or upon material model changes.

7. Administrative Safeguards

7.1 Sanctions Policy

- **Policy**: Sanction workforce for policy violations (45 CFR § 164.308(a)(1)(ii)(C)).
- **Procedures**:
  - Levels: 1 (accidental) – verbal warning; 2 (repeated) – written warning; 3 (intentional) – suspension; 4 (malicious) – termination.
  - Document incidents and allow appeals within 10 business days, resolved within 15 days.

7.2 Compliance Evaluation

- **Policy**: Periodically evaluate HIPAA compliance (45 CFR § 164.308(a)(8)).
- **Procedures**:
  - Use NIST 800-66 as a guide, with annual updates to control mappings.

- Conduct self-assessments, internal audits, and annual external reviews; remediate controls scoring <85%.
- Deploy automated monitoring tools with dashboards and retain evidence for six years.

7.3 Change Management

- **Policy**: Manage system changes to maintain security. Change evaluations may incorporate risk ratings, rollback preparedness, and safeguard preservation statements to support documentation requirements under 45 CFR §164.308(a)(8).
- **Procedures**:
  - Classify changes (Low/Medium/High) with escalating approvals (manager, Compliance Officer, Steering Committee).
  - Require security impact analysis and testing in separate environments for Medium/High changes.
  - Review post-implementation within 7 days.

7.3.1 Change Evaluation Best Practices

- **Purpose:** To strengthen audit readiness and support HIPAA Security Rule evaluations under **45 CFR §164.308(a)(8)**, Cognera Health documents additional change evaluation elements where appropriate.

a) Change Risk Rating

- **Description:** Each system or security change may be assigned a risk rating (Low, Medium, or High) to ensure review rigor is proportional to potential impact on PHI/ePHI.
- **Risk Rating Criteria:**
  - **Low:** No direct impact to PHI handling; no change to security safeguards
  - **Medium:** Modifies access controls, authentication, logging, encryption, or PHI workflows
  - **High:** Introduces new PHI data flows, vendors, AI models, or security architectures
- **Governance Alignment:** Supports **Section 7.3 (Change Management)** and **Section 9.1 (Risk Management)**.

b) Rollback Plan Reference

- **Description:** For Medium or High-risk changes, a rollback or recovery plan may be documented to ensure system availability and data integrity if unintended security or operational impacts occur.
- **Rollback Documentation May Include:**
  - Rollback plan reference ID
  - Trigger conditions (e.g., access failures, security anomalies)
  - Estimated rollback time objective
  - Post-rollback validation steps

- **HIPAA Alignment:** Supports **45 CFR §164.308(a)(7)** (Contingency Planning) and **§164.308(a)(8)** (Evaluation).

c) Safeguard Preservation Statement

- **Description:** Change documentation may include an explicit statement confirming whether existing administrative, technical, or physical safeguards were reduced, maintained, or enhanced as part of the change.
- **Audit Value:** Provides clear evidence that security protections were preserved.

8. Business Continuity and Disaster Recovery

- **Policy**: Ensure PHI/ePHI availability during disruptions (45 CFR § 164.308(a)(7)).
- **Procedures**:
  - Identify critical systems with RTOs (e.g., 4 hours) and RPOs (e.g., 15 minutes).
  - Maintain encrypted, geo-redundant backups tested quarterly.
  - Document recovery procedures with automated failover; test annually via simulations.
  - Notify Covered Entities within 24 hours of a reportable breach.

8.1 Emergency Mode Operations

- **Procedures**:
  - Use break-glass procedures with dual authorization, logged and reviewed post-event.
  - Maintain geo-redundant failover sites with tested SLAs.
  - Ensure redundant digital communication channels (e.g., cell, messaging apps).
  - Protect PHI with offline encryption during emergencies.

9. Risk Management

9.1 Risk Assessment and Management Policy for PHI/ePHI

- **Policy**: Identify and mitigate risks to PHI/ePHI (45 CFR § 164.308(a)(1)).
- **Procedures**:
  - Conduct annual risk assessments, scoring threats/vulnerabilities (low/medium/high).
  - Mitigate critical/high risks within 7/30 days; accept low/medium risks with justification (approved by Steering Committee for medium/high).
  - Assess third-party risks annually; require 24-hour incident reporting.
  - Monitor risks monthly with SIEM and update analysis after significant changes.

9.2 AI, Analytics, and Voice-to-Text Risk Management

- **Policy:** Cognera Health shall identify, assess, and mitigate risks associated with AI-driven analytics, predictive modeling, crisis monitoring, and voice-to-text technologies that process PHI/ePHI, in accordance with 45 CFR § 164.308(a)(1).
- **Procedures:**
  - Include AI models, analytics pipelines, and voice processing systems in annual HIPAA risk assessments.
  - Assess risks related to:
    - Data leakage
    - Model bias
    - False positives/negatives in crisis monitoring
    - Inaccurate transcription
  - Classify AI-related risks as low, medium, or high.
  - Remediate high-risk findings within 30 days.
  - Require third-party AI vendors to provide HIPAA assurances and BAAs.
  - Monitor AI system performance and anomalies continuously.
  - Reassess risks following:
    - Model retraining
    - Data source changes
    - New feature releases

10. Breach Notification and Incident Response

- **Policy**: Report and respond to breaches (45 CFR § 164.400-414) and security incidents (45 CFR § 164.308(a)(6)).
- **Procedures**:
  - Maintain 24/7 reporting channels; staff report to Compliance Officer within 1 hour.
  - Assess breaches within 72 hours using HIPAA's four-factor criteria (45 CFR § 164.402).
  - Notify Covered Entities within 24 hours, individuals/HHS within 60 days (media if >500 affected).
  - Contain, eradicate, and recover from incidents; review root causes within 14 days.
  - Log non-breach incidents (e.g., failed logins) and escalate per severity.

11. Training, Documentation, and Monitoring

11.1 HIPAA Training, Documentation, and Monitoring Policy

- **Training**: Require HIPAA training upon hire and annually, with an 85% passing score (45 CFR § 164.308(a)(5)).

- **Documentation**: Retain records (policies, logs, BAAs) for six years in an encrypted repository; include data deletion post-retention/contract termination (45 CFR § 164.316(b)(2)).
- **Monitoring**: Use CSPs/MSPs/MSSPs for 24/7 monitoring, quarterly internal audits, and annual external audits; review logs daily (alerts), weekly (access), and monthly (systems) (45 CFR § 164.308(a)(1)(ii)(D)).

11.2 AI and Voice-to-Text Documentation and Record Keeping

- **Policy:** Cognera Health shall maintain comprehensive documentation for AI, analytics, and voice-to-text processing activities involving PHI/ePHI to demonstrate compliance with HIPAA documentation requirements (45 CFR § 164.316).
- **Procedure:**
    - **Required Records (Retained for 6 Years):**
        - AI Model Data Use Disclosure
        - AI Risk & Bias Assessment Reports
        - AI Output Validation & Oversight Logs
        - Voice Recording Consent Forms (Provider and Client)
        - Audio-to-Text Data Retention and Deletion Logs
        - AI incident and anomaly reports
        - Vendor AI compliance attestations
    - **Monitoring:**
        - Review AI and voice-to-text logs monthly.
        - Conduct quarterly compliance reviews.
        - Escalate anomalies to the Compliance Officer within 24 hours.

12. Compliance KPIs

To evaluate and demonstrate HIPAA compliance effectiveness, the following KPIs are tracked:

KPI	Target	Frequency	Owner
HIPAA Training Completion Rate	≥95% within 30 days of hire / annually	Monthly	HR & Compliance
HIPAA Training Minimum Score to Pass	85%	Yearly	Compliance Officer
Time to Revoke Access Post-Termination	≤24 hours	Monthly	IT
High-Risk Security Patch Deployment	Within 7 days of identification	Monthly	IT Security
Breach Notification to Covered Entities	Within 24 hours	Per Incident	Compliance Officer
Access Review Completion	100%	Quarterly	Compliance Officer

Vendor BAA Compliance Attestation	100% compliance	Quarterly	Compliance Officer
Security Incident Mean Time to Detect (MTTD)	≤30 minutes	Monthly	MSSP / IT / Cloud
Security Incident Mean Time to Respond (MTTR)	≤60 minutes	Monthly	IT / Cloud
Audit Findings Closure Rate	100% of critical within 7 days, others within 30 days	Quarterly	Compliance / IT / Cloud

13. Continuous Improvement

- **Policy**: Update framework annually to address new threats and regulations (45 CFR § 164.308(a)(1)).
- **Procedures**: Incorporate audit findings, monitor OCR guidance, and benchmark against NIST/HITRUST.

14. Glossary

- **Workforce:** Employees, contractors, and third-party personnel, temporary staff and volunteers with access to PHI/ePHI
- **BA**: Business Associate – An entity that performs functions involving PHI on behalf of a Covered Entity.
- **BYOD**: Bring Your Own Device – Personal devices used for work purposes.
- **ePHI**: Electronic Protected Health Information – PHI in electronic form.
- **HIPAA**: Health Insurance Portability and Accountability Act – U.S. law governing healthcare data privacy and security.
- **MFA**: Multi-Factor Authentication – Security requiring multiple verification methods.
- **PHI**: Protected Health Information – Individually identifiable health information.
- **RBAC**: Role-Based Access Controls – Access limited by job function.
- **TLS**: Transport Layer Security – Protocol for secure data transmission.
- **TPO**: Treatment, Payment, and Healthcare Operations – Permitted uses of PHI under HIPAA.
- **CSP**: Cloud Service Provider
- **MSP**: Managed Service Provider
- **MSSP**: Managed Security Service Provider
- **NIST**: National Institute of Standards and Technology
- **SIEM**: Security Information and Event Management – Systems for real-time monitoring and analysis of security events.
- **HITRUST**: Health Information Trust Alliance
- **HITECH**: Health Information Technology for Economic and Clinical Health Act
- **RTO**: Timeframe to restore systems post-disruption (e.g., 4 hours for Heal Script).
- **RPO**: Maximum data loss tolerance (e.g., 15-minute backups).
- **OCR**: Office for Civil Rights (OCR)
- **HHS**: U.S. Department of Health and Human Services

- **Covered Entity:** A healthcare provider, health plan, or healthcare clearinghouse that transmits any health information in electronic form in connection with a HIPAA transaction. Cognera Health provides services on behalf of Covered Entities.
- **Security Incident:** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- **Safe Harbor (De-identification):** A method under the HIPAA Privacy Rule (45 CFR §164.514) that allows PHI to be considered de-identified when 18 specific identifiers are removed.
- **Expert Determination:** A method under HIPAA where a qualified expert determines, using statistical and
- **AI (Artificial Intelligence):** Systems or models that analyze data to generate insights, predictions, or recommendations in support of human decision-making.
- **Voice-to-Text:** Technology that converts spoken audio into written text, where audio or transcription may contain PHI/ePHI.
- **Human-in-the-Loop:** A governance model requiring human review, validation, or override of AI-generated outputs.

15. Conclusion

The Cognera Health™ Compliance Governance Framework establishes a comprehensive and scalable governance foundation for the protection, management, and responsible use of Protected Health Information (PHI), electronic Protected Health Information (ePHI), personal information, consumer health data, confidential business information, and other sensitive data across all Cognera Health platforms, services, systems, and operations.

This framework supports alignment with applicable healthcare regulations, privacy laws, cybersecurity standards, and industry-recognized governance frameworks, including HIPAA, HITECH, GDPR, UK GDPR, CCPA/CPRA, HITRUST CSF, ISO/IEC 27001, ISO/IEC 27701, SOC 2, NIST Cybersecurity Framework, and related regulatory and operational requirements. It provides the governance structures, policies, procedures, controls, and oversight mechanisms necessary to promote privacy, security, compliance, accountability, operational resilience, information governance, risk management, and responsible artificial intelligence practices.

Through continuous monitoring, risk assessment, workforce training, compliance oversight, governance reviews, security management, vendor oversight, and continuous improvement, Cognera Health maintains a risk-based and compliance-driven governance program designed to adapt to evolving regulatory obligations, customer requirements, emerging technologies, cybersecurity threats, healthcare industry expectations, and organizational growth.

By integrating privacy, security, compliance, operational excellence, and responsible AI governance into its core operating principles, Cognera Health remains committed to maintaining trust, safeguarding sensitive information, supporting healthcare organizations, and delivering secure, compliant, and innovative technology solutions that advance mental health, behavioral health, wellness, and continuous care delivery.

Approved By	Title	Signature	Date
Privacy Officer			
Compliance Officer			
CISO			
Legal Counsel			