CONFIDENTIAL | PROPRIETARY | RESTRICTED

Cognera Health™ Privacy & Data Protection Program

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.

Table of Contents

1. Purpose

1.1 Privacy Governance Charter

Purpose

The purpose of the Cognera Health™ Privacy & Data Protection Program is to establish a comprehensive governance framework governing the privacy, protection, confidentiality, integrity, availability, lawful processing, ethical use, retention, disclosure, sharing, transfer, archival, deletion, destruction, and stewardship of information throughout the organization.

This program serves as the authoritative privacy governance framework for Cognera Health and establishes enterprise-wide requirements governing the management of personal information, consumer health data, healthcare information, Protected Health Information (PHI), electronic Protected Health Information (ePHI), artificial intelligence processing data, voice and audio information, operational information, security information, and other regulated information.

This program is intended to provide a consistent, auditable, scalable, and sustainable framework supporting responsible information management throughout all products, services, technologies, business processes, workforce activities, vendor relationships, and operational functions.

Program Mission

The mission of the Cognera Health Privacy Program is to create and maintain a trusted healthcare technology environment in which information is managed responsibly, ethically, securely, transparently, and in accordance with applicable legal, regulatory, contractual, and organizational obligations.

The Privacy Program seeks to balance:

- Privacy Protection
- Information Security
- Clinical Operations
- Behavioral Health Operations
- Wellness Operations
- Artificial Intelligence Innovation

- Customer Requirements
- Regulatory Compliance
- Operational Effectiveness
- Responsible Data Use

The organization recognizes that privacy is not merely a compliance obligation but a foundational component of trust, organizational integrity, responsible innovation, and long-term business sustainability.

Privacy Vision

Cognera Health seeks to establish a privacy-conscious culture in which privacy considerations are integrated into every aspect of the organization.

The long-term vision is to maintain a mature privacy program capable of:

- Protecting individuals.
- Protecting healthcare organizations.
- Protecting providers.
- Protecting care teams.
- Protecting customers.
- Supporting responsible innovation.
- Supporting responsible artificial intelligence.
- Supporting regulatory readiness.
- Supporting enterprise growth.
- Supporting global operations.

The Privacy Program shall evolve continuously as technologies, regulations, customer expectations, healthcare practices, cybersecurity threats, and artificial intelligence capabilities evolve.

1.2 Privacy Objectives

The Privacy Program is intended to achieve the following objectives.

Protect Individual Privacy Rights

Protect privacy rights arising from:

- HIPAA

- HITECH
- GDPR
- UK GDPR
- CCPA
- CPRA
- Consumer Health Data Laws
- State Privacy Laws
- Emerging Privacy Regulations

Protect Sensitive Information

Protect throughout the information lifecycle:

- PHI
- ePHI
- Mental Health Information
- Behavioral Health Information
- Consumer Health Data
- Voice Information
- Audio Information
- Sensitive Personal Information
- Security Information

Support Regulatory Compliance

Maintain governance, controls, procedures, monitoring activities, and accountability mechanisms supporting applicable regulatory obligations.

Support Responsible Artificial Intelligence

Ensure AI technologies are deployed responsibly, ethically, transparently, and with appropriate human oversight.

Reduce Organizational Risk

Reduce following risks through effective governance and oversight:

- Privacy Risk
- Security Risk
- Regulatory Risk

- Legal Risk
- Operational Risk
- AI Risk
- Vendor Risk
- Reputational Risk

Support Enterprise Information Governance

Establish governance requirements governing of information:

- Collection
- Processing
- Storage
- Access
- Sharing
- Retention
- Deletion
- Disposal

1.3 Privacy Governance Philosophy

Cognera Health believes that privacy is a fundamental component of responsible healthcare technology operations.

The organization recognizes that individuals entrust healthcare organizations with highly sensitive information and that such trust must be protected through effective governance, strong security controls, responsible data stewardship, transparency, and accountability.

The Privacy Program is guided by the following beliefs:

Privacy Is a Fundamental Individual Right

Individuals should understand:

- What information is collected.
- Why information is collected.
- How information is processed.
- How information is shared.
- How information is retained.
- How information is protected.

Healthcare Information Requires Enhanced Protection

Healthcare information frequently contains highly sensitive personal information.

Examples include:

- Mental Health Information
- Behavioral Health Information
- Substance Use Information
- Crisis Intervention Information
- Wellness Information
- Treatment Information
- Assessment Information

Such information requires heightened governance, oversight, monitoring, accountability, and protection.

Transparency Builds Trust

Transparency is essential to maintaining trust among:

- Individuals
- Providers
- Organizations
- Customers
- Regulators
- Business Partners

Security Supports Privacy

Privacy cannot be effectively achieved without appropriate security controls.

Privacy protections depend upon:

- Administrative Safeguards
- Technical Safeguards
- Operational Safeguards
- Organizational Safeguards

Artificial Intelligence Requires Governance

Artificial intelligence creates opportunities and risks.

AI systems require:

- Human Oversight
- Accountability
- Transparency
- Explainability
- Validation
- Monitoring
- Risk Management
- Governance

1.4 Enterprise Data Stewardship Charter

Cognera Health acts as a steward of information entrusted to the organization.

Data stewardship responsibilities include:

- **Protection**
  - Protect information throughout its lifecycle.
- **Accountability**
  - Maintain clear ownership and responsibility.
- **Accuracy**
  - Promote information quality.
- **Integrity**
  - Protect information from unauthorized modification.
- **Availability**
  - Ensure authorized access when needed.
- **Confidentiality**
  - Protect information from unauthorized disclosure.
- **Responsible Use**
  - Use information only for legitimate purposes.
- **Regulatory Compliance**
  - Support applicable legal and regulatory obligations.
- **Ethical Use**
  - Promote ethical, fair, and responsible information processing practices.

1.5 Human Rights and Ethical Data Use Charter

Cognera Health recognizes that privacy protections support broader human rights principles.

The organization seeks to:

- Respect individual autonomy.
- Promote informed decision-making.
- Prevent misuse of information.
- Promote fairness.
- Promote transparency.
- Reduce discrimination risks.
- Reduce bias risks.
- Promote accountability.

These principles apply equally to:

- Human decision-making
- Automated processing
- Artificial intelligence systems
- Analytics systems
- Operational intelligence systems

1.6 Relationship to Enterprise Governance

The Privacy & Data Protection Program functions as a core component of the Cognera Health governance ecosystem.

This program shall operate in coordination with:

- Compliance Governance Framework
- Information Security Program
- Data Retention, Deletion, and Secure Disposal Policy
- Artificial Intelligence Governance Program
- Vendor Governance Program
- Incident Response Program
- Business Continuity Program
- Disaster Recovery Program
- HealScript™ Governance

- HealConnect™ Governance
- CogneraAI™ Governance

Where conflicts exist, the most restrictive privacy, security, legal, regulatory, or contractual requirement shall govern unless otherwise determined by Legal Counsel and the Data Governance Steering Committee.

2. Scope

2.1 Scope Statement

Purpose

The purpose of this section is to define the organizational, operational, technological, contractual, regulatory, geographic, workforce, vendor, information, and platform boundaries of the Cognera Health™ Privacy & Data Protection Program.

This section establishes the applicability of privacy governance requirements and identifies the individuals, technologies, business processes, information assets, services, and third-party relationships subject to this program.

The scope of this Privacy Program is intentionally broad to ensure privacy, security, compliance, information governance, retention, artificial intelligence governance, and data protection requirements are applied consistently throughout the organization.

Policy Statement

This Privacy & Data Protection Program applies to all information, systems, technologies, applications, services, personnel, vendors, business partners, contractors, subcontractors, service providers, operational processes, artificial intelligence systems, cloud environments, and business activities owned, operated, managed, developed, maintained, utilized, or otherwise controlled by Cognera Health™.

The requirements established by this program represent minimum privacy governance requirements.

Business units, products, customers, regulators, contractual obligations, or jurisdictions may impose additional requirements.

Where multiple requirements apply, the most restrictive requirement shall govern unless otherwise approved by Legal Counsel and the Data Governance Steering Committee.

2.2 Organizational Scope

Policy Statement

This Privacy Program applies to all organizational functions and business activities performed by or on behalf of Cognera Health.

Privacy requirements apply regardless of:

- Organizational structure
- Business unit
- Department
- Reporting relationship
- Physical location
- Technology environment

Corporate Functions

Privacy requirements apply to:

- **Executive Leadership**
  - Responsible for strategic governance, risk management, oversight, accountability, and Privacy sponsorship.
- **Product Management**
  - Responsible for privacy-by-design integration, feature governance, privacy requirements management, and privacy impact assessments.
- **Engineering**
  - Responsible for implementing privacy controls, security controls, retention controls, monitoring controls, and privacy requirements within technology solutions.
- **Operations**
  - Responsible for operational compliance, privacy process execution, vendor coordination, and service delivery.
- **Customer Success**
  - Responsible for supporting customer privacy requirements, customer requests, customer governance activities, and customer communications.
- **Compliance**

    - Responsible for compliance oversight, monitoring, audits, investigations, corrective actions, and regulatory readiness.
- **Privacy**
    - Responsible for privacy governance, privacy risk management, privacy rights, privacy investigations, privacy reviews, and privacy program administration.
- **Information Security**
    - Responsible for security governance supporting privacy objectives.
- **Legal**
    - Responsible for legal interpretation, contractual reviews, investigations, litigation support, and regulatory analysis.
- **Human Resources**
    - Responsible for workforce privacy requirements, training, personnel onboarding, workforce governance, and workforce termination procedures.

2.3 Platform Scope

Policy Statement

All Cognera Health products, platforms, applications, services, integrations, APIs, analytics systems, reporting systems, AI systems, and operational technologies fall within the scope of this Privacy Program.

HealScript™

Purpose

HealScript™ serves as Cognera Health's practitioner, provider, organizational management, documentation, operational intelligence, reporting, and workflow platform.

Privacy Scope

HealScript™ may process:

- PHI
- ePHI
- Clinical Records
- Assessments
- Treatment Plans
- Care Plans
- Care Coordination Records

- Scheduling Information
- Operational Data
- Reporting Data
- Analytics Data
- AI-Assisted Documentation

Governance Requirements

HealScript™ shall support:

- HIPAA Requirements
- Security Requirements
- Privacy Requirements
- Data Retention Requirements
- AI Governance Requirements
- Information Governance Requirements

HealConnect™

Purpose

HealConnect™ serves as Cognera Health's engagement, communication, wellness, behavioral health, journaling, assessment, and continuity-of-care platform.

Privacy Scope

HealConnect™ may process:

- Personal Information
- Consumer Health Data
- Behavioral Health Information
- Wellness Information
- Mood Tracking Information
- Journaling Information
- Assessment Information
- Voice Information
- Crisis Information
- Communications

Governance Requirements

HealConnect™ shall support:

- Privacy Requirements
- Security Requirements
- Consent Requirements
- Voice Processing Requirements
- Consumer Health Data Requirements
- AI Governance Requirements

CogneraAI™

Purpose

CogneraAI™ provides artificial intelligence, machine learning, NLP, NLU, workflow assistance, reporting, analytics, operational intelligence, engagement intelligence, and documentation capabilities.

Privacy Scope

CogneraAI™ may process:

- AI Inputs
- AI Outputs
- Clinical Information
- Behavioral Health Information
- Voice Transcriptions
- Communications
- Reports
- Analytics Information

Governance Requirements

CogneraAI™ shall support:

- AI Governance Requirements
- Human-in-the-Loop Requirements
- Privacy Requirements
- Security Requirements
- Monitoring Requirements
- Validation Requirements

2.4 Workforce Scope

Policy Statement

All individuals acting on behalf of Cognera Health are subject to this Privacy Program.

Privacy obligations apply regardless of employment status, contractual status, or location.

Employees

Includes:

- Full-Time Personnel
- Part-Time Personnel
- Temporary Personnel
- Seasonal Personnel

Contractors

Includes:

- Independent Contractors
- Consulting Personnel
- Contract Resources

Interns

Includes:

- Student Interns
- Graduate Interns
- Technical Interns

Volunteers

Includes:

- Authorized Volunteers
- Approved Program Participants

Workforce Obligations

All workforce members shall:

- Protect information.
- Complete training.

- Follow policies.
- Report incidents.
- Support privacy rights.
- Support audits.
- Support investigations.

2.5 Third-Party Scope

Policy Statement

Third parties processing information on behalf of Cognera Health are subject to applicable privacy, security, governance, contractual, and compliance requirements.

Cloud Service Providers (CSPs)

Examples include providers supporting:

- Hosting
- Storage
- Infrastructure
- Disaster Recovery

Managed Service Providers (MSPs)

Examples include providers supporting:

- Infrastructure
- Operations
- Administration
- Technical Services

Managed Security Service Providers (MSSPs)

Examples include providers supporting:

- Monitoring
- Security Operations
- Threat Detection
- Incident Response

Business Associates

Organizations performing functions involving PHI or ePHI.

Subcontractors

Organizations supporting contracted services.

AI Service Providers

Organizations supporting:

- NLP
- NLU
- AI Processing
- Machine Learning
- Voice Processing

2.6 Information Scope

Policy Statement

All information processed by Cognera Health falls within the scope of this Privacy Program.

Healthcare Information

Includes:

- PHI
- ePHI
- Clinical Records
- Mental Health Records
- Behavioral Health Records
- Substance Use Records
- Treatment Plans
- Care Plans

Consumer Health Information

Includes:

- Wellness Data
- Mood Tracking
- Recovery Activities
- Engagement Information
- Journaling Information

Personal Information

Includes:

- Identity Information
- Contact Information
- Sensitive Personal Information

Security Information

Includes:

- Audit Logs
- Security Logs
- Authentication Records
- Incident Records

Voice Information

Includes:

- Audio Files
- Voice Journals
- Voice Notes
- Voice-to-Text Data

AI Information

Includes:

- AI Inputs
- AI Outputs
- AI Governance Records
- AI Validation Records
- AI Monitoring Records

2.7 Geographic Scope

Policy Statement

This Privacy Program applies regardless of the geographic location where information is:

- Collected

- Processed
- Stored
- Shared
- Retained
- Accessed

Covered Locations

Includes:

- Corporate Environments
- Cloud Environments
- Remote Work Environments
- Vendor Environments
- Customer Environments
- International Processing Environments

2.8 Regulatory Scope

This Privacy Program supports governance activities arising from:

- HIPAA
- HITECH
- GDPR
- UK GDPR
- CCPA
- CPRA
- Consumer Health Data Laws
- State Privacy Laws
- BIPA
- Washington My Health My Data Act
- HITRUST
- ISO 27001
- ISO 27701
- NIST Guidance
- Applicable Healthcare Regulations

2.9 Technology Scope

Privacy requirements apply to:

Applications

- HealScript™
- HealConnect™
- APIs

Infrastructure

- Cloud Infrastructure
- Databases
- Storage Systems
- Backup Systems
- Disaster Recovery Systems

Analytics Platforms

- Reporting Platforms
- Analytics Platforms
- Intelligence Platforms

Artificial Intelligence Systems

- Machine Learning Models
- NLP Systems
- NLU Systems
- Recommendation Systems
- Predictive Models
- Voice Processing Systems

2.10 Scope Review and Maintenance

The scope of this Privacy Program shall be reviewed:

- Annually
- Following acquisitions
- Following divestitures
- Following major platform releases
- Following regulatory changes

- Following significant organizational changes

to ensure continued accuracy, completeness, and alignment with organizational operations.

Changes to scope shall be approved through established governance processes and documented within program governance records.

3. Regulatory Alignment, Legal Obligations, Standards Frameworks, and Compliance Governance

3.1 Purpose

Purpose Statement

The purpose of this section is to establish the regulatory, legal, contractual, compliance, privacy, cybersecurity, healthcare, information governance, records management, artificial intelligence governance, and operational governance requirements that inform the Cognera Health™ Privacy & Data Protection Program.

This section serves as the authoritative regulatory alignment framework supporting privacy, security, compliance, information governance, data protection, artificial intelligence governance, records management, and risk management activities throughout the organization.

Cognera Health recognizes that healthcare technology organizations operate within a highly regulated environment that requires continuous monitoring of healthcare laws, privacy regulations, cybersecurity requirements, artificial intelligence governance expectations, consumer protection requirements, contractual obligations, and industry-recognized frameworks.

The organization therefore maintains a governance model informed by multiple regulatory and standards-based requirements rather than relying upon a single regulatory framework.

3.2 Policy Statement

Cognera Health shall maintain privacy, security, compliance, information governance, records management, artificial intelligence governance, and operational control programs designed to support applicable requirements arising from:

- Healthcare Regulations
- Privacy Regulations
- Consumer Protection Requirements
- Consumer Health Data Regulations
- Cybersecurity Requirements
- Artificial Intelligence Governance Expectations
- Contractual Obligations
- Industry-Recognized Frameworks
- Organizational Governance Requirements

The organization shall continuously evaluate evolving requirements and adjust policies, controls, procedures, governance activities, monitoring activities, and operational practices where necessary.

3.3 Regulatory Governance Objectives

The objectives of Regulatory Alignment Governance are to:

- **Support Compliance**
  - Support compliance with applicable laws and regulations.
- **Support Risk Management**
  - Reduce privacy, security, legal, regulatory, and operational risks.
- **Support Customer Requirements**
  - Support enterprise customer due diligence, contractual obligations, and regulatory requirements.
- **Support Governance Maturity**
  - Establish repeatable and auditable governance processes.
- **Support Regulatory Readiness**
  - Maintain readiness for audits, reviews, investigations, assessments, and customer evaluations.
- **Support Continuous Improvement**
  - Continuously evaluate and improve governance activities.

3.4 Healthcare Regulatory Governance

Health Insurance Portability and Accountability Act (HIPAA)

Regulatory Overview

HIPAA establishes national standards governing the privacy, security, and protection of Protected Health Information (PHI).

As a Business Associate supporting Covered Entities, Cognera Health maintains controls designed to support applicable HIPAA obligations.

HIPAA influences nearly every aspect of the organization's privacy and security program.

Examples include:

- Privacy Governance
- Security Governance
- Access Management
- Authorization Management
- Information Sharing
- Disclosure Controls
- Vendor Oversight
- Risk Management
- Incident Response
- Retention Requirements
- Audit Activities

HIPAA Privacy Rule Governance

Purpose

The HIPAA Privacy Rule establishes standards governing:

- Uses of PHI
- Disclosures of PHI
- Individual Rights
- Authorization Requirements
- Minimum Necessary Requirements
- Administrative Requirements

Organizational Commitments

Cognera Health shall:

- Limit use of PHI to authorized purposes.
- Limit disclosure of PHI to authorized recipients.
- Support individual privacy rights.

- Support accounting of disclosures.
- Support authorization management.
- Support minimum necessary requirements.
- Maintain privacy safeguards.

Governance Activities

Examples include:

- Privacy Reviews
- Privacy Impact Assessments
- Disclosure Reviews
- Authorization Reviews
- Access Reviews
- Privacy Audits

HIPAA Security Rule Governance

Purpose

The HIPAA Security Rule establishes requirements governing protection of ePHI.

Administrative Safeguards

Examples include:

- Governance Programs
- Workforce Training
- Risk Assessments
- Vendor Oversight
- Security Policies
- Incident Response

Technical Safeguards

Examples include:

- Encryption
- MFA
- RBAC
- Logging
- Monitoring
- Authentication Controls

Operational Safeguards

Examples include:

- Disaster Recovery
- Backup Management
- Recovery Testing
- Business Continuity

Governance Objectives

Protect ePHI:

- Confidentiality
- Integrity
- Availability

HIPAA Breach Notification Rule

Purpose

Establish requirements governing:

- Breach Identification
- Investigation
- Notification
- Documentation
- Corrective Actions

Governance Requirements

Cognera Health shall maintain procedures supporting:

- Breach Analysis
- Incident Investigation
- Notification Support
- Corrective Action Tracking
- Lessons Learned Activities

3.5 HITECH Governance

Purpose

The HITECH Act strengthens healthcare privacy and security requirements and expands obligations applicable to Business Associates.

Governance Areas Influenced

Examples include:

- Breach Management
- Security Requirements
- Vendor Oversight
- Enforcement Activities
- Audit Readiness
- Compliance Documentation
- Risk Assessments

Organizational Commitments

Cognera Health shall:

- Protect PHI.
- Protect ePHI.
- Support Covered Entities.
- Support breach notification obligations.
- Maintain compliance documentation.

3.6 GDPR Governance

Purpose

The General Data Protection Regulation (GDPR) establishes privacy and data protection requirements governing personal data.

Where applicable, Cognera Health incorporates governance principles informed by GDPR requirements.

GDPR Governance Objectives

Support:

- Transparency
- Accountability
- Lawfulness

- Data Minimization
- Storage Limitation
- Individual Rights

Article 5 Governance Principles

- **Lawfulness, Fairness, and Transparency**
  - Processing activities shall be lawful, fair, and transparent.
- **Purpose Limitation**
  - Information shall be collected for specified and legitimate purposes.
- **Data Minimization**
  - Only necessary information shall be processed.
- **Accuracy**
  - Reasonable efforts shall be made to maintain accurate information.
- **Storage Limitation**
  - Information shall not be retained longer than necessary.
- **Integrity and Confidentiality**
  - Information shall be protected through appropriate safeguards.
- **Accountability**
  - Cognera Health shall maintain governance mechanisms demonstrating compliance.

Article 6 – Lawful Basis Governance

Where applicable, processing activities shall be supported by an appropriate lawful basis.

Examples include:

- Consent
- Contractual Necessity
- Legal Obligations
- Legitimate Interests
- Healthcare Activities

Article 9 – Special Category Data

Healthcare information, behavioral health information, biometric information, and related information may constitute special category data.

Additional safeguards shall be applied where appropriate.

Articles 15–21 Rights Governance

Support:

- Access
- Rectification
- Erasure
- Restriction
- Portability
- Objection

through established Privacy Rights Management procedures.

3.7 UK GDPR Governance

Cognera Health applies substantially similar governance principles where UK GDPR requirements apply.

Governance activities support:

- Transparency
- Individual Rights
- Accountability
- Data Protection
- Regulatory Compliance

3.8 California Privacy Governance

California Consumer Privacy Act (CCPA)

Governance Objectives

Support:

- Right to Know
- Right to Access
- Right to Delete
- Right to Information
- Non-Discrimination

California Privacy Rights Act (CPRA)

Governance Objectives

Support:

- Right to Correct
- Right to Limit Sensitive Personal Information
- Expanded Consumer Rights
- Increased Transparency

Sensitive Personal Information Governance

Sensitive information shall receive enhanced controls.

Examples include:

- Consumer Health Data
- Behavioral Health Information
- Mental Health Information
- Sensitive Identifiers

3.9 Consumer Health Data Governance

Cognera Health recognizes the emergence of specialized consumer health privacy laws.

Examples include:

- Washington My Health My Data Act
- Nevada Consumer Health Data Requirements
- Emerging State Privacy Laws

Governance activities shall evolve as laws evolve.

3.10 Biometric Privacy Governance

Illinois BIPA

Where applicable, Cognera Health shall support governance requirements related to:

- Notice
- Consent
- Retention Limitations
- Secure Disposal
- Restrictions on Sale
- Voiceprint Governance

- Biometric Information Protection

3.11 Texas Data Privacy and Security Act (TDPSA)

Where applicable, Cognera Health shall evaluate obligations arising from Texas privacy requirements.

Governance reviews shall evaluate:

- Data Collection
- Processing Activities
- Sharing Activities
- Consumer Rights
- Security Controls

3.12 New York SHIELD Act

Where applicable, Cognera Health shall evaluate:

- Security Requirements
- Privacy Requirements
- Breach Notification Requirements
- Data Protection Obligations

3.13 HITRUST Governance Alignment

Purpose

HITRUST provides a comprehensive healthcare-focused governance framework supporting privacy, security, compliance, risk management, and information governance activities.

Governance Areas

Examples include:

- Risk Management
- Information Protection
- Vendor Governance
- Access Management
- Incident Management

- Retention Governance

3.14 ISO/IEC 27001 Alignment

Cognera Health incorporates security governance principles informed by ISO 27001.

Examples include:

- Risk Management
- Security Governance
- Security Controls
- Continuous Improvement

3.15 ISO/IEC 27701 Alignment

Cognera Health incorporates privacy governance principles informed by ISO 27701.

Examples include:

- Privacy Governance
- Data Protection
- Privacy Management
- Individual Rights Support

3.16 SOC 2 Alignment

Cognera Health governance programs are informed by Trust Services Criteria including:

- Security
- Availability
- Confidentiality
- Processing Integrity
- Privacy

3.17 NIST Alignment

Cognera Health incorporates governance concepts informed by:

- **NIST Cybersecurity Framework**

    - Identify
    - Protect
    - Detect
    - Respond
    - Recover
- **NIST SP 800-53**
    - Security and Privacy Controls.
- **NIST SP 800-66**
    - HIPAA Security Rule Guidance.
- **NIST SP 800-88**
    - Media Sanitization and Secure Disposal.

3.18 Regulatory Monitoring Program

Policy Statement

Cognera Health shall maintain ongoing monitoring of:

- Healthcare Regulations
- Privacy Regulations
- AI Regulations
- Consumer Protection Laws
- Cybersecurity Requirements
- Industry Frameworks

Monitoring Activities

Examples include:

- Regulatory Reviews
- Legal Reviews
- Compliance Reviews
- Governance Reviews
- Industry Monitoring
- Vendor Monitoring

Escalation

Significant regulatory developments shall be escalated where appropriate:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Data Governance Steering Committee
- Executive Leadership

3.19 Regulatory Readiness Program

Cognera Health shall maintain readiness for:

- Regulatory Reviews
- Customer Assessments
- Security Reviews
- Privacy Reviews
- Compliance Audits
- Due Diligence Activities
- Vendor Assessments
- AI Governance Reviews

3.20 Continuous Improvement

Regulatory alignment activities shall be reviewed periodically to improve:

- Compliance Readiness
- Privacy Governance
- Security Governance
- AI Governance
- Risk Management
- Regulatory Monitoring

The objective is to maintain a mature, auditable, scalable, and continuously improving governance program capable of supporting evolving regulatory requirements and healthcare technology operations.

4. Privacy Governance Program

4.1 Privacy Governance Charter

Purpose

The purpose of the Privacy Governance Program is to establish the organizational framework through which privacy, data protection, information governance, privacy risk management, privacy compliance, privacy operations, privacy rights management, artificial intelligence governance, and privacy accountability are directed, managed, monitored, measured, audited, and continuously improved.

The Privacy Governance Program serves as the central coordinating mechanism for all privacy-related activities across Cognera Health™ and provides the structure necessary to ensure that privacy obligations are consistently addressed throughout products, services, technologies, business processes, vendor relationships, workforce activities, and operational functions.

This program is intended to transform privacy from a compliance activity into a strategic governance capability supporting organizational trust, responsible innovation, operational excellence, customer confidence, regulatory readiness, and enterprise risk management.

Policy Statement

Cognera Health shall maintain a formal Privacy Governance Program that:

- Establishes privacy accountability.
- Defines governance authority.
- Assigns responsibilities.
- Supports privacy risk management.
- Supports regulatory compliance.
- Supports privacy-by-design.
- Supports responsible AI governance.
- Supports information lifecycle governance.
- Supports customer trust.
- Supports enterprise decision-making.

Privacy governance activities shall be integrated into all organizational activities involving information.

Privacy governance shall not operate independently of security governance, compliance governance, AI governance, records governance, vendor governance, or operational governance.

4.2 Privacy Governance Mission

The mission of the Privacy Governance Program is to ensure that privacy considerations are systematically incorporated into organizational decision-making, technology development, information management, service delivery, vendor management, and business operations.

The Privacy Governance Program seeks to create an environment where:

- Privacy is understood.
- Privacy is respected.
- Privacy is monitored.
- Privacy is measured.
- Privacy is auditable.
- Privacy is continuously improved.

The organization recognizes that privacy governance is a continuous discipline requiring active oversight and organizational commitment.

4.3 Privacy Governance Objectives

The Privacy Governance Program shall support the following objectives.

Privacy Protection

Protect individuals from:

- Unauthorized disclosure
- Unauthorized access
- Excessive collection
- Improper processing
- Unnecessary retention
- Unauthorized sharing

Regulatory Compliance

Support compliance with:

- HIPAA

- HITECH
- GDPR
- UK GDPR
- CCPA
- CPRA
- Consumer Health Data Laws
- State Privacy Laws
- Emerging Privacy Requirements

Enterprise Risk Management

Support identification, assessment, mitigation, monitoring, reporting, and management of privacy-related risks.

Responsible Technology Use

Support:

- Ethical AI
- Responsible Analytics
- Responsible Automation
- Responsible Data Use

Organizational Accountability

Ensure accountability exists for:

- Privacy Decisions
- Privacy Controls
- Privacy Risks
- Privacy Incidents
- Privacy Obligations

4.4 Privacy Governance Framework

The Privacy Governance Framework consists of multiple interconnected governance domains.

Governance Domain 1

Privacy Management

Responsible for:

- Privacy Policies
- Privacy Procedures
- Privacy Standards
- Privacy Controls

Governance Domain 2

Information Governance

Responsible for:

- Classification
- Ownership
- Stewardship
- Lifecycle Management

Governance Domain 3

Privacy Rights Management

Responsible for:

- Access Requests
- Deletion Requests
- Correction Requests
- Restriction Requests

Governance Domain 4

Consent Governance

Responsible for:

- HIPAA Authorizations
- AI Consent
- Voice Consent
- Telehealth Consent

Governance Domain 5

AI Governance

Responsible for:

- AI Oversight

- AI Validation
- AI Monitoring
- AI Risk Management

Governance Domain 6

Vendor Governance

Responsible for:

- Vendor Privacy Reviews
- Vendor Monitoring
- Vendor Risk Management

Governance Domain 7

Privacy Risk Management

Responsible for:

- Risk Assessments
- Risk Monitoring
- Risk Reporting

4.5 Privacy Governance Structure

Privacy governance shall be supported through a multi-layer governance model.

Executive Leadership

Executive leadership provides:

- Strategic Oversight
- Resource Allocation
- Risk Acceptance Authority
- Governance Sponsorship

Executive leadership maintains ultimate accountability for the effectiveness of the Privacy Program.

Privacy Officer

The Privacy Officer serves as the primary operational authority responsible for privacy governance.

Responsibilities include:

- Program Leadership
- Privacy Oversight
- Privacy Risk Management
- Privacy Reviews
- Privacy Rights Management
- Privacy Reporting
- Privacy Investigations

Compliance Officer

The Compliance Officer supports:

- Regulatory Readiness
- Compliance Monitoring
- Auditing Activities
- Corrective Actions
- Compliance Reporting

Chief Information Security Officer

The CISO supports as part of privacy governance activities:

- Security Governance
- Security Risk Management
- Security Monitoring
- Security Incident Response

Legal Counsel

Legal Counsel supports:

- Regulatory Interpretation
- Contract Reviews
- Legal Holds
- Investigations
- Litigation Support

Data Governance Steering Committee

The Steering Committee provides enterprise governance oversight.

Responsibilities include:

- Policy Approval

- Risk Oversight
- Governance Reviews
- AI Governance Reviews
- Retention Governance Reviews

4.6 Privacy Governance Authority

Privacy governance authority shall be exercised according to documented authority matrices.

Authority areas include:

- Policy Approval
- Risk Acceptance
- Exception Approval
- AI Deployment Approval
- Vendor Approval
- Data Sharing Approval
- Privacy Rights Decisions
- Regulatory Response Decisions

No privacy-related authority shall be assumed without documented delegation or governance assignment.

4.7 Privacy Risk Management Program

Purpose

The Privacy Risk Management Program is intended to identify, evaluate, prioritize, mitigate, monitor, and report privacy-related risks.

Privacy Risk Categories

Examples include:

- **Regulatory Risk**
  - Failure to comply with applicable requirements.
- **Security Risk**
  - Unauthorized access, disclosure, or misuse.
- **Operational Risk**

    - Failures in processing activities.
- **Vendor Risk**
    - Third-party privacy failures.
- **AI Risk**
    - Improper AI processing.
- **Voice Processing Risk**
    - Improper voice collection or disclosure.
- **Reputational Risk**
    - Loss of trust.

Risk Assessment Activities

Privacy risks shall be evaluated through:

- Privacy Risk Assessments
- Privacy Impact Assessments
- Vendor Reviews
- AI Reviews
- Security Reviews
- Governance Reviews

4.8 Privacy Impact Assessment Program

Policy Statement

Cognera Health shall maintain a Privacy Impact Assessment (PIA) Program.

Purpose

PIAs evaluate privacy implications associated with:

- New Products
- New Services
- New Technologies
- New Integrations
- New Vendors
- New AI Systems

Assessment Areas

Examples include:

- Information Collected
- Information Shared
- Retention Requirements
- Consent Requirements
- Privacy Risks
- Security Risks
- AI Risks
- Regulatory Impacts

Approval Requirements

PIAs may require review by:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Security Leadership

4.9 Data Protection Impact Assessment Program

Where required, Cognera Health may perform DPIAs.

DPIAs may be conducted for:

- High-Risk Processing
- AI Systems
- Behavioral Health Data
- Consumer Health Data
- Large-Scale Processing Activities

4.10 Privacy Governance Reviews

Privacy governance activities shall undergo periodic review.

Monthly Reviews

Examples include:

- Rights Requests
- Complaints
- Consent Activities

Quarterly Reviews

Examples include:

- Privacy Metrics
- Risk Assessments
- Governance Activities
- Vendor Reviews

Annual Reviews

Examples include:

- Program Effectiveness
- Regulatory Alignment
- Policy Reviews
- Governance Maturity

4.11 Privacy Governance Reporting

Governance reporting shall be provided to appropriate stakeholders.

Executive Leadership Reporting

Examples include:

- Privacy Risks
- Significant Incidents
- Governance Effectiveness
- Strategic Privacy Issues

Steering Committee Reporting

Examples include:

- Privacy Metrics
- Risk Metrics
- AI Governance Findings
- Audit Findings

Compliance Reporting

Examples include:

- Compliance Findings
- Corrective Actions
- Regulatory Developments

4.12 Privacy Governance Metrics

Examples include:

- Privacy Incidents
- Privacy Complaints
- Privacy Rights Requests
- Vendor Privacy Reviews
- AI Governance Reviews
- Consent Activities
- Risk Assessments
- Audit Findings

Governance Objectives

Metrics are intended to support:

- Accountability
- Transparency
- Continuous Improvement
- Executive Oversight

4.13 Privacy Auditing Program

Privacy governance activities shall be subject to periodic auditing.

Examples include:

- Internal Privacy Audits
- Compliance Audits
- Vendor Audits
- AI Governance Audits
- Privacy Rights Audits
- Retention Audits

Audit Objectives

Evaluate:

- Compliance
- Control Effectiveness
- Governance Effectiveness
- Risk Exposure

4.14 Privacy Exception Management

Policy Statement

Privacy exceptions shall be formally managed.

Requirements

Exceptions shall:

- Be documented.
- Include business justification.
- Include risk assessment.
- Include compensating controls.
- Include expiration dates.
- Include approval records.

Approval Authority

Exceptions shall be approved according to documented authority matrices.

4.15 Continuous Improvement

The Privacy Governance Program shall be continuously improved through:

- Audit Findings
- Incident Reviews
- Risk Assessments
- Regulatory Monitoring
- Vendor Reviews
- AI Governance Reviews
- Customer Feedback

- Governance Maturity Assessments

The objective is to maintain a mature, auditable, scalable, risk-aware, privacy-conscious, and continuously improving Privacy governance program supporting all Cognera Health operations, technologies, products, and services.

5. Privacy Principles

5.1 Purpose

Purpose Statement

The purpose of this section is to establish the foundational privacy principles that guide all information governance, privacy, security, compliance, artificial intelligence, operational, business, and technology activities throughout Cognera Health™.

These principles serve as the philosophical, ethical, operational, and governance foundation for all privacy-related decisions, policies, procedures, controls, standards, technologies, and organizational activities.

The Privacy Principles defined in this section shall be applied consistently throughout:

- Product Development
- Service Delivery
- Information Governance
- Artificial Intelligence Systems
- Vendor Relationships
- Operational Activities
- Customer Engagement
- Data Management
- Security Activities

These principles shall guide both human decision-making and automated processing activities.

5.2 Policy Statement

Cognera Health shall apply privacy principles throughout the entire information lifecycle.

Privacy principles shall guide all information processed by the organization:

- Collection
- Creation
- Processing
- Storage
- Access
- Use
- Sharing
- Disclosure
- Analytics
- Artificial Intelligence
- Retention
- Deletion
- Destruction

Privacy principles apply regardless of:

- Technology platform
- Information type
- Data source
- Customer
- Geography
- Regulatory jurisdiction
- Vendor relationship

These principles establish minimum governance expectations applicable throughout the organization.

5.3 Transparency Principle

Principle Statement

Individuals, customers, providers, care teams, organizations, regulators, and other stakeholders should be able to reasonably understand how information is collected, processed, used, shared, retained, protected, and governed.

Transparency is essential to maintaining trust and supporting informed decision-making.

Objectives

The Transparency Principle seeks to:

- Promote trust.
- Reduce uncertainty.
- Improve understanding.
- Support privacy rights.
- Support informed consent.
- Improve accountability.

- **Transparency Requirements**
  - Cognera Health shall provide reasonable transparency regarding:
- **Information Collection**
  - What information is collected.
- **Information Use**
  - How information is used.
- **Information Sharing**
  - Who information is shared with.
- **Retention Practices**
  - How long information is retained.
- **Artificial Intelligence**
  - When AI is used and how it supports processing activities.
- **Voice Processing**
  - When voice technologies are used.
- **Privacy Rights**
  - Available privacy rights and request mechanisms.

Transparency Mechanisms

Examples include:

- Privacy Notices
- Consent Forms
- Privacy Policies
- Terms & Conditions
- EULA Documents
- AI Disclosures
- Point-of-Use Notices

- Customer Documentation

5.4 Purpose Limitation Principle

Principle Statement

Information shall be collected, processed, used, retained, disclosed, shared, and otherwise managed only for authorized, documented, legitimate, and appropriate purposes.

Information shall not be processed for unrelated purposes without an appropriate legal basis, authorization, consent, contractual requirement, regulatory obligation, or other lawful justification.

Objectives

Purpose limitation supports:

- Privacy Protection
- Accountability
- Compliance
- Transparency
- Risk Reduction

Requirements

Every significant processing activity should have:

- Defined Purpose
- Documented Purpose
- Approved Purpose
- Governed Purpose

Examples

- **Authorized Purpose**
  - Collecting assessment data to support treatment planning.
- **Unauthorized Purpose**
  - Using assessment data for unrelated activities without authorization.

5.5 Data Minimization Principle

Principle Statement

Cognera Health shall collect, process, store, share, retain, and use only the minimum amount of information reasonably necessary to accomplish authorized purposes.

The organization shall avoid excessive collection, excessive retention, excessive sharing, and excessive processing.

Objectives

Data minimization supports:

- Privacy Protection
- Security Protection
- Compliance
- Risk Reduction

Collection Requirements

Only information necessary shall be collected:

- Care Delivery
- Care Coordination
- Operations
- Security
- Compliance
- Contractual Obligations

Processing Requirements

Processing activities should be limited to information reasonably necessary to support the approved purpose.

Retention Requirements

Information shall not be retained solely because storage capacity exists.

Retention requires documented justification.

5.6 Accuracy Principle

Principle Statement

Cognera Health shall make reasonable efforts to ensure that information remains accurate, complete, relevant, reliable, and current.

Information quality directly impacts:

- Care Delivery
- Decision-Making
- Analytics
- AI Outputs
- Reporting
- Compliance Activities

Objectives

Support:

- Reliable Information
- Trustworthy Information
- Quality Reporting
- Effective Operations

Accuracy Activities

Examples include:

- Validation
- Quality Reviews
- Correction Processes
- User Review
- Provider Review
- AI Validation

Correction Requirements

Mechanisms shall exist to support correction of inaccurate information where appropriate.

5.7 Storage Limitation Principle

Principle Statement

Information shall not be retained longer than necessary to satisfy:

- Clinical Requirements
- Regulatory Requirements
- Legal Requirements
- Contractual Requirements
- Security Requirements
- Operational Requirements

Objectives

Support:

- Data Minimization
- Privacy Protection
- Security Protection
- Compliance

Requirements

Information shall be approved according to the retention schedules:

- Retained appropriately.
- Archived appropriately.
- Deleted appropriately.
- Destroyed appropriately.

5.8 Confidentiality Principle

Principle Statement

Information shall be protected from unauthorized access, unauthorized disclosure, unauthorized sharing, unauthorized exposure, and unauthorized use.

Confidentiality protections apply regardless of:

- Information format
- Storage location
- Processing location

Objectives

Protect from privacy harm:

- Individuals
- Customers
- Providers
- Care Teams
- Organizations

Confidentiality Controls

Examples include:

- Access Controls
- Encryption
- Authentication
- Monitoring
- Vendor Controls
- Secure Disposal

5.9 Integrity Principle

Principle Statement

Information shall be protected against unauthorized modification, corruption, manipulation, destruction, alteration, or degradation.

Objectives

Ensure information remains:

- Accurate
- Reliable
- Complete
- Trustworthy

Integrity Controls

Examples include:

- Version Control
- Audit Logging
- Validation
- Change Management
- Access Controls

5.10 Availability Principle

Principle Statement

Authorized users should have timely access to information when needed for legitimate purposes.

Objectives

Support:

- Care Delivery
- Care Coordination
- Operations
- Compliance
- Security Activities

Availability Controls

Examples include:

- Backup Systems
- Disaster Recovery
- Business Continuity
- Monitoring
- Redundancy
- Recovery Testing

5.11 Accountability Principle

Principle Statement

Privacy obligations require clear ownership, responsibility, oversight, monitoring, and accountability.

Objectives

Support:

- Governance
- Oversight

- Transparency
- Auditability
- Compliance

Accountability Activities

Examples include:

- Policy Management
- Governance Reviews
- Audits
- Risk Assessments
- Reporting
- Corrective Actions

5.12 Privacy by Design Principle

Principle Statement

Privacy considerations shall be incorporated into systems, technologies, processes, products, and services from the earliest stages of planning and development.

Privacy should be proactive rather than reactive.

Applicability

Privacy by Design applies to:

- Product Development
- System Design
- AI Development
- Integrations
- APIs
- Vendor Selection
- Operational Processes

Requirements

Privacy reviews may be required during:

- Design
- Development

- Testing
- Deployment
- Operational Changes

5.13 Security by Design Principle

Principle Statement

Security controls shall be incorporated into systems, products, services, and technologies from inception through retirement.

Objectives

Support:

- Confidentiality
- Integrity
- Availability

Security by Design Activities

Examples include:

- Secure Development
- Threat Modeling
- Security Testing
- Vulnerability Reviews
- Penetration Testing

5.14 Responsible Artificial Intelligence Principle

Principle Statement

Artificial Intelligence systems shall be deployed responsibly and with appropriate governance.

Objectives

Support:

- Transparency
- Explainability

- Accountability
- Fairness
- Privacy
- Security

Governance Requirements

AI systems shall support:

- Human-in-the-Loop Oversight
- Validation
- Monitoring
- Bias Reviews
- Risk Management
- Auditing

5.15 Ethical Data Use Principle

Principle Statement

Information shall be used responsibly, ethically, fairly, and in a manner consistent with organizational values and applicable obligations.

Objectives

Promote:

- Fairness
- Trust
- Accountability
- Responsible Innovation

Ethical Considerations

Examples include:

- Bias Reduction
- Transparency
- Respect for Individual Rights
- Responsible AI

- Appropriate Data Use

5.16 Continuous Improvement Principle

Principle Statement

Privacy governance shall continuously evolve to address:

- Regulatory Changes
- Technology Changes
- Security Threats
- Customer Expectations
- AI Developments
- Industry Best Practices

Improvement Activities

Examples include:

- Audits
- Assessments
- Reviews
- Monitoring
- Incident Reviews
- Regulatory Reviews

Governance Objective

Maintain a mature, scalable, auditable, privacy-conscious, and continuously improving privacy program capable of supporting the long-term mission and growth of Cognera Health™.

6. Roles, Responsibilities, Accountability, Authority, Oversight, and Governance Ownership

6.1 Purpose

Purpose Statement

The purpose of this section is to establish clear accountability, ownership, authority, responsibilities, governance obligations, oversight mechanisms, escalation paths, segregation-of-duties requirements, and decision-making authority for all privacy, data protection, information governance, artificial intelligence governance, security governance, records management, compliance, and risk management activities throughout Cognera Health™.

This section establishes who is responsible, accountable, consulted, and informed regarding privacy-related activities and provides the governance structure necessary to support regulatory compliance, risk management, operational effectiveness, customer trust, and organizational accountability.

The organization recognizes that privacy governance cannot be effective without clearly assigned ownership and accountability.

Every privacy obligation, privacy control, privacy process, privacy risk, privacy decision, and privacy activity shall have an identified owner.

6.2 Policy Statement

Cognera Health shall maintain clearly defined privacy, security, compliance, information governance, artificial intelligence governance, records management, and operational governance responsibilities across the organization.

Responsibilities shall be assigned according to:

- Job Function
- Governance Role
- Access Level
- Operational Authority
- Regulatory Obligations
- Risk Ownership
- Decision-Making Authority

Privacy accountability remains a shared responsibility throughout the organization; however, specific governance activities shall have designated accountable owners.

No governance activity shall exist without assigned ownership.

6.3 Governance Accountability Model

Cognera Health utilizes a multi-layer governance accountability model.

Strategic Governance Layer

Responsible for:

- Strategy
- Governance Direction
- Resource Allocation
- Enterprise Risk Oversight

Executive Governance Layer

Responsible for:

- Enterprise Accountability
- Governance Sponsorship
- Risk Acceptance
- Organizational Prioritization

Operational Governance Layer

Responsible for:

- Privacy Operations
- Compliance Operations
- Security Operations
- Vendor Governance

Oversight Layer

Responsible for:

- Monitoring
- Auditing
- Validation
- Risk Evaluation

Execution Layer

Responsible for:

- Day-to-Day Activities
- Control Operation
- Policy Compliance
- Incident Reporting

6.4 Executive Leadership Responsibilities

Role Purpose

Executive Leadership maintains ultimate accountability for the effectiveness of the Privacy & Data Protection Program.

Executive Leadership is responsible for ensuring privacy governance receives appropriate organizational support, funding, authority, visibility, and strategic alignment.

Responsibilities

Executive Leadership shall:

- **Governance Sponsorship**
  - Provide active support for privacy governance activities.
- **Resource Allocation**
  - Allocate resources necessary to support privacy, compliance, and security activities.
- **Enterprise Risk Oversight**
  - Review significant privacy, compliance, security, AI, and vendor risks.
- **Strategic Direction**
  - Ensure privacy governance aligns with organizational objectives.
- **Regulatory Readiness**
  - Support organizational readiness for audits, investigations, customer reviews, and regulatory inquiries.
- **Culture**
  - Promote a culture supporting privacy, accountability, transparency, and ethical information management.

Authority

Executive Leadership may:

- Accept Privacy risk.
- Approve Privacy strategy.
- Approve Privacy investments.
- Approve major governance initiatives.
- Escalate matters to ownership or the Board (if applicable).

6.5 Privacy Officer

Role Purpose

The Privacy Officer serves as the primary operational authority responsible for privacy governance throughout the organization.

The Privacy Officer is accountable for the design, implementation, oversight, monitoring, measurement, and continuous improvement of the Privacy Program.

Responsibilities

Governance Leadership

Develop and maintain:

- Privacy Policies
- Privacy Standards
- Privacy Procedures
- Privacy Controls

Privacy Risk Management

Coordinate:

- Privacy Risk Assessments
- Privacy Reviews
- Privacy Impact Assessments
- Data Protection Impact Assessments

Privacy Rights Management

Oversee:

- Access Requests
- Deletion Requests
- Correction Requests
- Restriction Requests

- Complaints
- Appeals

Consent Governance

Review:

- HIPAA Authorizations
- AI Consents
- Voice Consents
- Telehealth Consents

Privacy Incident Management

Coordinate:

- Privacy Investigations
- Breach Reviews
- Corrective Actions

Reporting

Provide:

- Privacy Metrics
- Privacy Risk Reports
- Governance Reports

Authority

The Privacy Officer may:

- Require corrective actions.
- Suspend privacy-noncompliant activities.
- Escalate privacy concerns.
- Request audits.
- Require privacy reviews.

6.6 Compliance Officer

Role Purpose

The Compliance Officer is responsible for compliance governance supporting privacy and data protection objectives.

Responsibilities

Regulatory Monitoring

Monitor:

- HIPAA
- HITECH
- GDPR
- CCPA
- State Privacy Laws
- Consumer Health Data Laws

Auditing

Coordinate:

- Internal Audits
- Compliance Reviews
- Corrective Actions

Regulatory Readiness

Support:

- Investigations
- Assessments
- Regulatory Reviews

Compliance Reporting

Provide compliance reporting to leadership.

Authority

The Compliance Officer may:

- Initiate compliance reviews.
- Require remediation plans.
- Escalate compliance concerns.

6.7 Chief Information Security Officer (CISO)

Role Purpose

The CISO is responsible for information security governance supporting privacy and data protection requirements.

Responsibilities

Security Governance

Maintain:

- Security Policies
- Security Standards
- Security Controls

Security Risk Management

Conduct:

- Security Assessments
- Vulnerability Assessments
- Threat Assessments

Security Monitoring

Oversee:

- SIEM Operations
- Security Monitoring
- Threat Detection

Incident Response

Coordinate:

- Security Investigations
- Security Incidents
- Breach Response

Authority

The CISO may:

- Approve security controls.
- Require remediation.
- Restrict access.

- Escalate security concerns.

6.8 Legal Counsel

Role Purpose

Legal Counsel provides legal oversight supporting privacy, security, compliance, information governance, AI governance, vendor governance, and risk management activities.

Responsibilities

Legal Interpretation

Interpret:

- HIPAA
- HITECH
- GDPR
- CCPA
- State Privacy Laws

Contract Reviews

Review:

- BAAs
- DPAs
- Vendor Contracts
- Customer Agreements

Legal Holds

Coordinate:

- Legal Holds
- Preservation Requirements
- eDiscovery

Investigations

Support:

- Regulatory Investigations

- Litigation
- Enforcement Activities

Authority

Legal Counsel may:

- Issue legal holds.
- Approve legal disclosures.
- Approve subpoena responses.
- Escalate legal risks.

6.9 Data Governance Steering Committee

Purpose

The Steering Committee serves as the highest standing governance authority for information governance activities.

Responsibilities

Governance Oversight

Review:

- Privacy Programs
- Security Programs
- AI Governance Programs
- Vendor Governance Programs

Policy Approval

Approve:

- Privacy Policies
- Governance Policies
- Retention Schedules

Risk Oversight

Review:

- Privacy Risks
- Security Risks

- AI Risks
- Vendor Risks

Metrics Oversight

Review:

- Privacy Metrics
- Compliance Metrics
- Security Metrics
- AI Metrics

Authority

The Steering Committee may:

- Approve governance policies.
- Approve high-risk exceptions.
- Review enterprise risks.
- Direct corrective actions.

6.10 Data Owners

Policy Statement

All information assets shall have designated ownership.

Data Owners are accountable for governance and lifecycle management of assigned information assets.

Clinical Data Owner

Responsible for:

- Clinical Records
- Assessments
- Treatment Plans
- Care Plans
- Care Coordination Records

Authority

Approve:

- Access Requirements
- Retention Requirements
- Disposition Activities

Privacy Data Owner

Responsible for:

- Consent Records
- Authorization Records
- Privacy Requests
- Disclosure Records

Security Data Owner

Responsible for:

- Audit Logs
- Authentication Logs
- Incident Records
- Security Records

AI Governance Data Owner

Responsible for:

- AI Inventories
- Validation Records
- AI Monitoring Records
- AI Risk Assessments

6.11 Product Leadership

Product Leadership shall:

- Implement Privacy by Design.
- Support Security by Design.
- Participate in PIAs.
- Participate in AI Governance Reviews.
- Participate in Vendor Reviews.

6.12 Engineering Leadership

Engineering Leadership shall:

- Implement privacy controls.
- Implement security controls.
- Support secure development.
- Support vulnerability remediation.
- Support privacy reviews.

6.13 Operations Leadership

Operations Leadership shall:

- Support privacy compliance.
- Support retention activities.
- Support incident management.
- Support vendor governance.

6.14 Workforce Responsibilities

Every workforce member shall:

- Protect Information
- Follow Policies
- Complete Training
- Report Incidents
- Report Concerns
- Support Privacy Rights
- Support Compliance Activities
- Support Audits
- Support Investigations

6.15 Vendor Responsibilities

Vendors shall:

- Protect information.
- Follow contractual requirements.

- Support audits.
- Support privacy reviews.
- Support security reviews.
- Support incident response.

6.16 Business Associate Responsibilities

Business Associates shall:

- Comply with BAAs.
- Protect PHI.
- Protect ePHI.
- Report incidents.
- Support investigations.
- Support audits.

6.17 Governance Authority Matrix

Governance Activity	Privacy Officer	Compliance Officer	CISO	Legal Counsel	Steering Committee	Executive Leadership
Privacy Policy Approval	Recommend	Review	Review	Review	Approve	Ratify
Retention Schedule Approval	Review	Review	Review	Review	Approve	Ratify
Privacy Rights Denials	Approve	Review	N/A	Review	Escalate if High Risk	N/A
AI Governance Policy	Review	Review	Review	Review	Approve	Ratify
Vendor Privacy Exception	Review	Review	Review	Review	Approve	Escalate if High Risk
High Risk Privacy Exception	Recommend	Review	Review	Review	Review	Approve
Regulatory Response	Review	Review	Review	Approve	Inform	Inform

Breach Notification	Review	Review	Review	Approve	Inform	Inform

6.18 Segregation of Duties

Where practical SofD shall remain separate:

- Approval authority
- Implementation authority
- Oversight authority
- Audit authority

No individual should simultaneously:

- Approve a control
- Operate a control
- Audit the same control

6.19 Escalation Authority

The following matters shall be escalated immediately:

- Critical Privacy Incidents
- Significant Data Breaches
- OCR Investigations
- Regulatory Investigations
- High-Risk AI Incidents
- High-Risk Vendor Incidents
- Legal Hold Events
- Litigation Events
- Executive Risk Matters

6.20 RACI Governance Framework

The organization shall maintain detailed RACI matrices for:

- Privacy Governance
- AI Governance
- Vendor Governance

- Rights Management
- Incident Response
- Retention Governance
- Security Governance
- Regulatory Response

These matrices shall identify parties for all major governance activities:

- Responsible
- Accountable
- Consulted
- Informed

6.21 Annual Responsibility Review

Roles, responsibilities, authorities, delegations, and governance assignments shall be reviewed:

- Annually
- Following organizational changes
- Following regulatory changes
- Following significant incidents
- Following major audits

to ensure ongoing effectiveness, accountability, and governance maturity.

The objective is to maintain a clear, auditable, accountable, and scalable governance model supporting all privacy and data protection activities throughout the Cognera Health ecosystem.

7. Information Categories, Data Classification, Information Ownership, Data Stewardship, and Information Governance

7.1 Purpose

Purpose Statement

The purpose of this section is to establish a comprehensive enterprise information governance framework governing the classification, categorization, ownership, stewardship, handling, protection, monitoring, retention, disclosure, sharing, archival, deletion, destruction, and lifecycle management of information processed by Cognera Health™.

Information is one of the organization's most critical assets. Effective information governance is necessary to ensure that information is:

- Protected appropriately.
- Classified consistently.
- Used responsibly.
- Retained appropriately.
- Shared lawfully.
- Managed securely.
- Governed effectively.
- Disposed of properly.

This section establishes the foundation upon which privacy controls, security controls, retention controls, AI governance controls, disclosure controls, and compliance obligations are applied.

7.2 Policy Statement

Cognera Health shall classify, categorize, govern, protect, monitor, retain, disclose, archive, de-identify, anonymize, delete, destroy, and otherwise manage information according to:

- Sensitivity
- Regulatory Requirements
- Privacy Requirements
- Security Requirements
- Confidentiality Requirements
- Business Value
- Operational Impact
- Risk Profile
- Customer Requirements
- Contractual Obligations

Information governance activities shall support:

- Privacy Protection
- Security Protection
- Regulatory Compliance
- Risk Management
- Information Quality
- Responsible AI
- Business Continuity
- Accountability

All information processed by Cognera Health shall be assigned an appropriate classification and ownership designation.

7.3 Information Governance Objectives

The Information Governance Program seeks to:

- **Protect Sensitive Information**
  - Protect healthcare, behavioral health, consumer health, and personal information.
- **Support Regulatory Compliance**
  - Support privacy, healthcare, cybersecurity, and records management requirements.
- **Improve Information Quality**
  - Promote accurate, reliable, complete, and trustworthy information.
- **Support Responsible AI**
  - Ensure information used by AI systems is governed appropriately.
- **Improve Accountability**
  - Establish ownership and stewardship responsibilities.
- **Support Lifecycle Governance**
  - Ensure information is governed throughout its lifecycle.

7.4 Information Governance Principles

Information governance activities shall support:

- **Privacy**

- Protecting individual privacy rights.

- **Security**
  - Protecting information assets.
- **Accountability**
  - Maintaining clear ownership and responsibility.
- **Availability**
  - Supporting authorized access.
- **Integrity**
  - Protecting information quality.
- **Compliance**
  - Supporting legal and regulatory obligations.
- **Stewardship**
  - Managing information responsibly.
- **Transparency**
  - Providing visibility into information practices.
- **Responsible AI**
  - Supporting ethical AI processing activities.

7.5 Information Classification Framework

Policy Statement

Cognera Health maintains a four-tier information classification model.

All information assets shall be classified according to sensitivity, confidentiality, privacy requirements, regulatory requirements, and risk.

Classification determines:

- Access Controls
- Security Controls
- Monitoring Controls
- Sharing Restrictions
- Retention Requirements
- Disposal Requirements

Restricted Information

Definition

Restricted Information represents the highest level of sensitivity.

Unauthorized access, disclosure, use, modification, destruction, or loss could result in:

- Significant Privacy Harm
- Regulatory Penalties
- Legal Exposure
- Financial Loss
- Reputational Damage
- Customer Harm
- Clinical Harm

Examples

- **Healthcare Information**
  - PHI
  - ePHI
  - Clinical Records
  - Mental Health Records
  - Behavioral Health Records
  - Substance Use Records
  - Crisis Intervention Records
- **Personal Information**
  - Sensitive Personal Information
  - Consumer Health Data
  - Government Identifiers
  - Biometric Information
- **Security Information**
  - Authentication Credentials
  - Security Keys
  - Encryption Keys
  - Security Incident Records
- **AI Governance Information**
  - AI Validation Reports
  - AI Risk Assessments
  - AI Monitoring Records

Control Requirements

Restricted information shall require:

- Encryption at Rest
- Encryption in Transit
- MFA
- RBAC
- Audit Logging
- Monitoring
- Retention Controls
- Secure Disposal Controls
- Vendor Restrictions
- Enhanced Review Requirements

Confidential Information

Definition

Confidential Information includes sensitive operational, contractual, business, governance, and security-related information.

Examples

- Contracts
- Financial Records
- Audit Reports
- Vendor Information
- Governance Records
- Risk Assessments
- Product Roadmaps

Required Controls

Examples include:

- Access Controls
- Encryption
- Monitoring
- Retention Controls

Internal Information

Definition

Information intended for internal organizational use.

Examples

- Procedures
- Internal Communications
- Administrative Records
- Training Materials

Required Controls

Examples include:

- Access Controls
- Monitoring
- Retention Controls

Public Information

Definition

Information approved for public disclosure.

Examples

- Website Content
- Marketing Content
- Public Reports
- Press Releases

Requirements

Public information shall be reviewed prior to publication.

7.6 Information Ownership Framework

Policy Statement

Every information asset shall have an assigned owner.

Ownership establishes accountability for:

- Classification
- Access Approval
- Quality Oversight

- Retention Requirements
- Disposal Approval
- Regulatory Compliance

Information Owner Responsibilities

Information Owners shall:

- Classify Information
- Approve Access
- Review Retention
- Approve Disposal
- Support Audits
- Support Investigations
- Review Quality
- Review Risks

7.7 Data Stewardship Framework

Purpose

Data stewards support day-to-day governance and management of information assets.

Responsibilities

Data Stewards may:

- Monitor Data Quality
- Support Audits
- Support Reporting
- Support Privacy Reviews
- Support Retention Activities
- Support AI Governance Reviews

7.8 Identity Information Governance

Definition

Identity Information includes information capable of identifying, authenticating, or distinguishing an individual.

Examples

- Full Name
- Username
- User Identifier
- Employee Identifier
- Provider Identifier
- NPI Number
- Government ID
- Professional License Number

Collection Requirements
Identity information shall be collected only when necessary.

Access Requirements
Access restricted to authorized personnel.

Sharing Requirements
Sharing limited to authorized purposes.

Retention Requirements
Retention according to approved schedules.

Disposal Requirements
Secure deletion and disposal required.

7.9 Contact Information Governance

Examples

- Email Address
- Phone Number
- Mailing Address
- Emergency Contact Information

Purpose

Support:

- Communications
- Notifications
- Scheduling

- Customer Support
- Controls
- Access Controls
- Encryption
- Monitoring
- Retention Controls

7.10 Healthcare Information Governance

Policy Statement

Healthcare information requires enhanced protections.

Categories

- Clinical Documentation
- Behavioral Health Information
- Mental Health Information
- Substance Use Information
- Care Coordination Information
- Treatment Information
- Assessment Information

Regulatory Considerations

May be subject to:

- HIPAA
- HITECH
- State Healthcare Laws
- Behavioral Health Laws
- Substance Use Regulations

Governance Requirements

Healthcare information shall support:

- Enhanced Access Controls
- Enhanced Monitoring
- Enhanced Auditing

- Enhanced Retention Controls
- Enhanced Disposal Controls

7.11 Assessment Information Governance

Examples

- PHQ-9
- GAD-7
- OQ-45.2
- C-SSRS
- PCL-5
- AUDIT
- DAST
- WHO-5
- Custom Assessments

Purpose

Support:

- Screening
- Monitoring
- Outcome Measurement
- Treatment Planning

Governance Requirements

Assessment information shall support:

- Accuracy Reviews
- Quality Controls
- Provider Review
- Auditability

7.12 Consumer Health Data Governance

Definition

Consumer health data includes information related to health, wellness, mood, behavior, recovery, symptoms, and self-reported experiences.

Examples

- Mood Tracking
- Wellness Tracking
- Recovery Activities
- Symptom Tracking
- Journaling Activities

Governance Requirements

Consumer health data shall support:

- Consent Controls
- Privacy Controls
- Access Controls
- Retention Controls
- Deletion Controls

7.13 Voice and Audio Information Governance

Examples

- Voice Journals
- Voice Notes
- Audio Recordings
- Transcriptions
- Dictation

Regulatory Considerations

May be subject to:

- HIPAA
- BIPA
- State Recording Laws
- Consumer Health Data Laws

Governance Requirements

- Consent Controls
- Encryption
- Monitoring
- Retention Controls
- Secure Disposal

7.14 Artificial Intelligence Information Governance

Examples

- AI Inputs
- AI Outputs
- Validation Records
- Monitoring Records
- Human Review Records
- AI Risk Assessment

Governance Requirements

AI information shall support:

- Logging
- Validation
- Monitoring
- Auditing
- Risk Reviews
- Human Oversight

7.15 Security Information Governance

Examples

- Audit Logs
- Security Logs
- Authentication Records
- Incident Records
- Vulnerability Reports

Governance Requirements

Security information shall support:

- Integrity Protection
- Access Controls
- Monitoring
- Retention Controls
- Investigation Support

7.16 Information Lifecycle Governance

Policy Statement

All information categories shall be governed throughout:

- Collection
- Creation
- Processing
- Storage
- Access
- Use
- Sharing
- Disclosure
- Archival
- Retention
- Deletion
- Destruction
- Final Disposition

Governance Objective

Ensure information remains protected throughout its lifecycle.

7.17 Information Quality Governance

Objectives

Maintain information that is:

- Accurate
- Complete

- Consistent
- Reliable
- Relevant
- Timely

Quality Activities

Examples include:

- Validation
- Review
- Error Correction
- Monitoring
- Auditing

7.18 Information Governance Metrics

Examples include:

- Classification Compliance
- Ownership Assignment Rates
- Data Quality Findings
- Access Review Completion
- Retention Compliance
- Disposal Compliance
- AI Governance Findings

7.19 Monitoring and Auditing

Information governance activities shall be monitored and audited periodically.

Examples include:

- Classification Reviews
- Access Reviews
- Quality Reviews
- Retention Audits
- AI Governance Reviews

- Security Audits

7.20 Continuous Improvement

Information governance activities shall be continuously improved through:

- Audits
- Assessments
- Reviews
- Incident Findings
- Regulatory Reviews
- AI Governance Reviews

The objective is to maintain a mature, scalable, auditable, and enterprise-grade information governance program supporting all information assets processed by Cognera Health™.

8. Data Collection Sources, Collection Methods, Collection Controls, Information Acquisition Governance, and Data Collection Risk Management

8.1 Purpose

Purpose Statement

The purpose of this section is to establish enterprise governance requirements governing the collection, acquisition, creation, receipt, generation, ingestion, import, synchronization, recording, and capture of information throughout the Cognera Health™ ecosystem.

Data collection activities represent the first stage of the information lifecycle and therefore create significant privacy, security, regulatory, operational, artificial intelligence, and reputational risks if not properly governed.

This section establishes the controls, requirements, approvals, validations, monitoring activities, auditing requirements, accountability mechanisms, and governance expectations applicable to all information collection activities.

The organization recognizes that privacy risks often originate at the point of collection.

Accordingly, information shall be collected only when there is a legitimate, authorized, documented, and approved purpose.

8.2 Policy Statement

Cognera Health shall collect, receive, create, acquire, generate, record, import, synchronize, process, or otherwise obtain information only for legitimate and authorized purposes.

Information collection activities shall support:

- Privacy Protection
- Data Minimization
- Purpose Limitation
- Transparency
- Accountability
- Regulatory Compliance
- Security Protection
- Responsible AI Governance

Information shall not be collected merely because collection is technically possible.

Collection activities must be justified, documented, governed, monitored, and subject to periodic review.

8.3 Data Collection Governance Objectives

The Data Collection Governance Program seeks to:

Protect Privacy

Reduce privacy risks associated with excessive or inappropriate collection.

Reduce Risk

Reduce:

- Privacy Risk
- Security Risk

- Regulatory Risk
- Operational Risk
- AI Risk

Improve Transparency
Ensure individuals understand collection activities.

Support Compliance
Support regulatory obligations governing collection.

Support Data Quality
Promote collection of accurate and useful information.

Support Responsible AI
Ensure AI systems receive appropriately governed inputs.

8.4 Collection Governance Principles

All collection activities shall support the following principles.

Purpose Limitation

Information shall be collected only for:

- Authorized Purposes
- Documented Purposes
- Approved Purposes
- Legitimate Purposes

Every significant collection activity should have a documented business, operational, clinical, legal, regulatory, security, compliance, or customer purpose.

Data Minimization

Only the minimum information reasonably necessary to accomplish the intended purpose shall be collected.

Examples include:

Appropriate Collection

Collecting to support care delivery:

- Name

- Contact Information
- Assessment Responses

Excessive Collection

Collecting information unrelated to and excessive collection is prohibited.:

- Care Delivery
- Operations
- Security
- Compliance

Transparency

Individuals should understand:

- What information is collected.
- Why information is collected.
- How information is used.
- How information is shared.
- How information is retained.

Accountability

Collection activities shall have assigned ownership.

Every significant collection process shall have:

- Business Owner
- Data Owner
- Privacy Oversight

Security

Collection activities shall incorporate safeguards protecting information during acquisition and transmission.

8.5 Collection Authority Requirements

Policy Statement

No significant collection activity shall occur without appropriate authority and approval.

Collection Authority Sources

Examples include:

- Customer Authorization
- Contractual Requirements
- Regulatory Requirements
- Organizational Requirements
- User Consent
- HIPAA Authorizations
- Operational Requirements

Collection Documentation

Collection activities shall be documented.

Documentation may include:

- Purpose
- Information Collected
- Source
- Legal Basis
- Retention Requirements
- Sharing Activities

8.6 Direct Collection from Individuals

Policy Statement

Cognera Health may collect information directly from individuals through authorized interactions.

Collection Sources

Examples include:

- Registration Activities
- Intake Activities
- Assessments
- Journaling
- Messaging
- Wellness Activities
- Voice Activities

- Consent Activities

Information Types

Examples include:

- Personal Information
- Consumer Health Data
- Behavioral Health Information
- Assessment Information
- Voice Information
- Communications

Controls

Direct collection activities shall support:

- Transparency
- Consent
- Validation
- Security
- Monitoring

8.7 Collection from Providers

Policy Statement

Providers may contribute information through HealScript™ and related workflows.

Examples

- Clinical Notes
- Assessments
- Treatment Plans
- Care Plans
- Care Coordination Activities
- Clinical Documentation

Governance Requirements

Provider collection activities shall support:

- Documentation Standards
- Clinical Governance
- Privacy Controls
- Security Controls

8.8 Collection from Healthcare Organizations

Policy Statement

Cognera Health may receive information from Covered Entities and healthcare organizations.

Sources

Examples include:

- Clinics
- Behavioral Health Organizations
- Wellness Organizations
- Health Systems
- Hospitals
- Provider Groups

Governance Requirements

Healthcare organization collection activities shall support:

- HIPAA Requirements
- Customer Requirements
- Contractual Requirements
- Security Requirements

8.9 HealScript™ Collection Governance

Purpose

Support:

- Documentation
- Assessments

- Care Coordination
- Treatment Planning
- Operational Intelligence

Collection Activities

Examples include:

- Clinical Documentation
- Assessments
- Scheduling Activities
- Reporting Activities
- Care Coordination Activities

Governance Requirements

HealScript™ collection activities shall support:

- RBAC
- Logging
- Monitoring
- Consent Requirements
- Data Quality Controls

8.10 HealConnect™ Collection Governance

Purpose

Support:

- Engagement
- Wellness
- Recovery
- Journaling
- Assessments
- Communications

Collection Activities

Examples include:

- Mood Tracking

- Wellness Tracking
- Journaling
- Voice Journaling
- Messaging
- Assessments

Governance Requirements

HealConnect™ collection activities shall support:

- Transparency
- Consent
- Security
- Data Minimization
- Monitoring

8.11 CogneraAI™ Collection Governance

Policy Statement

CogneraAI™ may receive information from authorized workflows.

Examples

- Clinical Notes
- Assessments
- Journals
- Voice Transcriptions
- Communications
- Reports

Governance Requirements

AI-related collection activities shall support:

- Human Oversight
- Transparency
- Validation
- Monitoring
- Audit Logging

8.12 Voice and Audio Collection Governance

Policy Statement

Voice and audio information shall be collected only where authorized, necessary, and appropriate.

Examples

- Voice Journals
- Voice Notes
- Clinical Dictation
- Telehealth Audio
- Recorded Sessions

Consent Requirements

Where applicable:

- Voice Consent
- Recording Consent
- AI Consent
- Telehealth Consent

Controls

Voice collection activities shall support:

- Encryption
- Monitoring
- Retention Controls
- Disposal Controls

8.13 Automated Collection Governance

Policy Statement

Certain information may be collected automatically.

Examples

- Authentication Logs
- Access Logs

- Security Events
- API Activity
- Usage Metrics
- Device Information
- Performance Metrics

Governance Requirements

Automated collection shall support:

- Transparency
- Security
- Monitoring
- Auditability

8.14 Third-Party Collection Governance

Policy Statement

Information received from third parties shall be subject to governance review.

Examples

- Vendors
- APIs
- Integrations
- Healthcare Systems
- Referral Sources

Requirements

Third-party collection activities shall support:

- Contractual Requirements
- Privacy Requirements
- Security Requirements
- Data Quality Requirements

8.15 Collection Validation Program

Policy Statement

Collected information shall undergo validation appropriate to its purpose and sensitivity.

Validation Activities

Examples include:

- Completeness Validation
- Format Validation
- Identity Validation
- Authorization Validation
- Integrity Validation
- Quality Validation

Objectives

Improve collected information:

- Accuracy
- Reliability
- Trustworthiness

8.16 Collection Risk Management

Policy Statement

Collection activities shall be evaluated for privacy, security, compliance, operational, and AI-related risks.

Risk Categories

- Excessive Collection
- Unauthorized Collection
- Undisclosed Collection
- AI Collection Risks
- Voice Collection Risks
- Regulatory Risks

Risk Mitigation Activities

Examples include:

- Privacy Reviews
- Security Reviews
- AI Reviews
- Vendor Reviews
- Impact Assessments

8.17 Prohibited Collection Activities

Cognera Health prohibits:

- **Unauthorized Collection**
  - Collection without authorization.
- **Excessive Collection**
  - Collection exceeding legitimate needs.
- **Unlawful Collection**
  - Collection violating legal or regulatory requirements.
- **Undisclosed Collection**
  - Collection without appropriate transparency.
- **Unauthorized Recording**
  - Recording without required authorization.
- **Unauthorized AI Collection**
  - Collection outside approved AI governance requirements.

8.18 Collection Monitoring Program

Collection activities shall be monitored periodically.

Monitoring Areas

Examples include:

- Collection Volume
- Collection Sources
- Consent Compliance
- Voice Collection
- AI Collection
- Vendor Collection

Monitoring Objectives

Identify:

- Risks
- Anomalies
- Noncompliance
- Governance Gaps

8.19 Collection Auditing Program

Collection activities shall be periodically audited.

Audit Areas

Examples include:

- Transparency Compliance
- Consent Compliance
- Data Minimization Compliance
- AI Collection Compliance
- Voice Collection Compliance
- Vendor Collection Compliance

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Control Effectiveness

8.20 Collection Metrics

Examples include:

- Collection Compliance Rate
- Consent Capture Rate
- Validation Success Rate
- Collection Exceptions
- Collection Audit Findings
- AI Collection Findings

- Voice Collection Findings

8.21 Collection Documentation Requirements

Documentation shall be maintained regarding:

- Collection Purposes
- Collection Sources
- Collection Methods
- Consent Requirements
- Retention Requirements
- Regulatory Requirements
- AI Requirements
- Sharing Requirements

Retention

Documentation shall be retained according to approved retention schedules.

8.22 Continuous Improvement

Collection governance activities shall be periodically reviewed to improve:

- Privacy Protection
- Security Protection
- Transparency
- Data Quality
- Governance Maturity
- AI Governance
- Regulatory Readiness

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Major Platform Changes

The objective is to maintain a mature, auditable, privacy-conscious, secure, and compliant collection governance program supporting all information acquisition activities throughout the Cognera Health ecosystem.

9. Data Processing Activities, Information Use, Information Handling, Processing Governance, and Data Management Controls

9.1 Purpose

Purpose Statement

The purpose of this section is to establish enterprise governance requirements governing the processing, use, handling, transformation, storage, access, sharing, disclosure, analysis, aggregation, reporting, artificial intelligence processing, retention, deletion, and management of information throughout the Cognera Health™ ecosystem.

Information processing represents the operational use of information after collection and is one of the highest-risk activities within a privacy program because improper processing may result in:

- Unauthorized disclosures
- Privacy violations
- Regulatory violations
- Security incidents
- AI governance failures
- Customer harm
- Reputational damage

This section establishes the governance framework through which all information processing activities shall be controlled, monitored, reviewed, audited, and continuously improved.

9.2 Policy Statement

Cognera Health shall process information only for legitimate, authorized, documented, approved, contractual, operational, healthcare, clinical, compliance, security, legal, regulatory, or customer-directed purposes.

All processing activities shall support:

- Privacy Protection
- Security Protection
- Accountability
- Transparency
- Data Minimization
- Purpose Limitation
- Regulatory Compliance
- Responsible AI Governance

Information shall not be processed in a manner inconsistent with. Unauthorized processing is prohibited:

- Applicable Law
- Customer Agreements
- Business Associate Agreements
- Data Processing Agreements
- Organizational Policies
- Approved Processing Purposes

9.3 Data Processing Governance Objectives

The Data Processing Governance Program seeks to:

- **Protect Privacy**
  - Ensure information is processed appropriately.
- **Reduce Risk**
  - Reduce privacy, security, regulatory, operational, and AI-related risks.
- **Support Compliance**
  - Support healthcare, privacy, security, and contractual requirements.
- **Improve Accountability**
  - Establish ownership and oversight.

- **Improve Data Quality**
  - Support reliable information processing.
- **Support Responsible AI**
  - Ensure AI processing activities remain governed.
- **Support Operational Excellence**
  - Promote effective and efficient processing activities.

9.4 Processing Lifecycle Governance

Policy Statement

All information shall be governed throughout its lifecycle.

Lifecycle Stages

- **Collection**
  - Obtaining information from authorized sources.
- **Creation**
  - Generating information through approved activities.
- **Processing**
  - Using information for authorized purposes.
- **Storage**
  - Maintaining information within approved environments.
- **Access**
  - Retrieving information through authorized access controls.
- **Use**
  - Supporting healthcare, operational, security, compliance, and business activities.
- **Sharing**
  - Providing information to authorized recipients.
- **Disclosure**
  - Releasing information under approved circumstances.
- **Analytics**
  - Generating insights, reports, metrics, and intelligence.
- **Retention**
  - Maintaining information according to approved schedules.
- **Deletion**
  - Removing information when eligible.

- **Destruction**
  - Secure disposal of information.
- **Final Disposition**
  - Completion of lifecycle management activities.

9.5 Authorized Processing Purposes

Policy Statement

Information shall be processed only for approved purposes.

Healthcare Purposes

Examples include:

- Care Delivery
- Care Coordination
- Treatment Planning
- Outcome Measurement
- Clinical Documentation
- Follow-Up Activities

Operational Purposes

Examples include:

- Scheduling
- Reporting
- Analytics
- Workflow Management
- Performance Monitoring
- Operational Intelligence

Security Purposes

Examples include:

- Authentication
- Threat Detection
- Monitoring
- Security Investigations

- Incident Response

Compliance Purposes

Examples include:

- Audits
- Investigations
- Regulatory Reporting
- Risk Assessments
- Governance Reviews

AI Purposes

Examples include:

- Documentation Assistance
- Summarization
- Reporting Assistance
- Analytics
- Workflow Assistance

9.6 Information Use Governance

Policy Statement

Use of information shall be restricted to authorized individuals performing authorized activities.

Authorized Users

Examples include where appropriate:

- **Providers**
- **Care Teams**
- **Administrators**
- **Compliance Personnel**
- **Security Personnel**
- **Operations Personnel**
- **Authorized Vendors**

Use Restrictions

Information shall not be:

- Used Without Authorization
- Used Outside Approved Purposes
- Used for Personal Benefit
- Used in Violation of Customer Requirements
- Used in Violation of Regulatory Requirements

Minimum Necessary Principle

Information use shall be limited to the minimum information reasonably necessary to accomplish the authorized purpose.

9.7 Information Storage Governance

Policy Statement

Information shall be stored only in approved environments.

Approved Storage Locations

Examples include:

- Production Systems
- Clinical Systems
- Operational Systems
- Backup Systems
- Disaster Recovery Systems
- Analytics Platforms
- Reporting Platforms
- Secure Archives

Storage Requirements

Storage environments shall support:

- Encryption
- Access Controls
- Monitoring
- Logging
- Retention Controls

- Disposal Controls

9.8 Access Governance

Policy Statement

Access shall be granted only to authorized individuals where appropriate.

- Access Principles
- Least Privilege
- Need-to-Know
- Role-Based Access
- Segregation of Duties
- Just-In-Time Access

Access Controls

Examples include:

- RBAC
- MFA
- Conditional Access
- Session Controls
- Logging
- Monitoring

Access Reviews

Access reviews shall occur:

- Quarterly
- Following Role Changes
- Following Terminations
- Following Incidents

9.9 Information Sharing Governance

Policy Statement

Information sharing shall occur only when:

- Authorized

- Necessary
- Appropriate
- Documented

Authorized Recipients

Examples include where legally authorized:

- Covered Entities
- Providers
- Care Teams
- Business Associates
- Vendors
- Regulatory Authorities
- Law Enforcement

Sharing Controls

Examples include:

- Minimum Necessary
- Access Controls
- Encryption
- Logging
- Monitoring
- Authorization Validation

9.10 Analytics Governance

Policy Statement

Analytics activities shall support legitimate operational, healthcare, compliance, reporting, quality improvement, and business objectives.

Analytics Activities

Examples include:

- Operational Analytics
- Clinical Analytics
- Behavioral Analytics

- Engagement Analytics
- Outcome Analytics
- Enterprise Analytics
- AI Analytics

Governance Requirements

Analytics activities shall support:

- Data Minimization
- Privacy Controls
- Security Controls
- Governance Oversight
- Monitoring

9.11 Reporting Governance

Policy Statement

Reporting activities shall support authorized business, healthcare, operational, compliance, and customer objectives.

Report Types

Examples include:

- Clinical Reports
- Outcome Reports
- Operational Reports
- KPI Reports
- Executive Reports
- Compliance Reports
- AI Reports

Reporting Controls

Reports shall support:

- Access Controls
- Distribution Controls

- Privacy Controls
- Auditability

9.12 Artificial Intelligence Processing Governance

Policy Statement

AI-enabled processing activities require enhanced governance.

AI Processing Activities

Examples include:

- Documentation Assistance
- Summarization
- Recommendations
- Analytics
- Workflow Automation
- Reporting

AI Governance Requirements

AI processing shall support:

- Human Review
- Validation
- Monitoring
- Logging
- Auditing
- Risk Management

Restrictions

AI outputs shall not replace:

- Clinical Judgment
- Professional Judgment
- Regulatory Obligations

9.13 Automated Processing Governance

Policy Statement

Certain processing activities may be automated.

Automation shall not eliminate:

- Oversight
- Accountability
- Governance
- Validation
- Monitoring

Examples

- Notifications
- Scheduling
- Messaging
- Workflow Routing
- Reporting
- AI Activities

Monitoring Requirements

Automated processing activities shall be monitored periodically.

9.14 Human Review Governance

Policy Statement

Human review remains a critical governance control.

Human Review Activities

Examples include:

- AI Validation
- Documentation Review
- Reporting Review
- Risk Review
- Governance Review

Escalation

Concerns identified through review activities shall be escalated according to established governance procedures.

9.15 Data Quality Governance

Policy Statement

Cognera Health shall maintain controls supporting information quality.

Data Quality Objectives

- Accuracy
- Completeness
- Consistency
- Integrity
- Reliability
- Timeliness

Data Quality Activities

Examples include:

- Validation Rules
- Human Review
- Automated Checks
- Error Correction
- Quality Audits

9.16 Data Transformation Governance

Policy Statement

Information may be transformed to support authorized processing activities.

Examples

- Voice-to-Text
- Structured Documentation
- AI Summarization
- Analytics Transformation
- Reporting Transformation

Requirements

Transformation activities shall support:

- Validation
- Monitoring
- Auditability
- Data Integrity

9.17 Aggregation Governance

Policy Statement

Information may be aggregated to support:

- Reporting
- Analytics
- Operational Intelligence
- Quality Improvement

Governance Requirements

Aggregation activities shall support:

- Privacy Protection
- Security Protection
- Data Minimization
- Regulatory Compliance

9.18 De-Identification Governance

Policy Statement

Information may be de-identified where appropriate.

Purposes

Examples include:

- Analytics
- Reporting

- Product Improvement
- Research
- AI Governance

Requirements

De-identification shall support:

- HIPAA Requirements
- Privacy Requirements
- Security Requirements
- Governance Reviews

9.19 Anonymization Governance

Policy Statement

Information may be anonymized where appropriate and legally permissible.

Objectives

- Risk Reduction
- Privacy Protection
- Research Support
- Analytics Support

Controls

Anonymization activities shall be documented and subject to review.

9.20 Processing Risk Management

Policy Statement

Processing activities shall be evaluated for privacy, security, compliance, operational, vendor, and AI-related risks.

Risk Categories

- Unauthorized Processing
- Excessive Processing
- Improper Sharing

- AI Risks
- Vendor Risks
- Security Risks
- Regulatory Risks

Risk Mitigation Activities

Examples include:

- Privacy Reviews
- Security Reviews
- Vendor Reviews
- AI Reviews
- Impact Assessments

9.21 Processing Monitoring Program

Processing activities shall be monitored periodically.

Monitoring Areas

Examples include:

- Access Activities
- Sharing Activities
- AI Activities
- Vendor Activities
- Security Events
- Compliance Events

Monitoring Objectives

Identify:

- Noncompliance
- Anomalies
- Excessive Processing
- Unauthorized Activities

9.22 Processing Auditing Program

Processing activities shall be audited periodically.

Audit Areas

Examples include:

- Privacy Audits
- Compliance Audits
- Security Audits
- AI Audits
- Vendor Audits
- Retention Audits

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Control Effectiveness
- Risk Exposure

9.23 Processing Metrics

Examples include:

- Access Review Completion
- AI Validation Rates
- Processing Exceptions
- Audit Findings
- Data Quality Findings
- Privacy Incidents
- Security Incidents

9.24 Processing Exceptions

Policy Statement

Processing activities outside approved purposes require:

- Privacy Review
- Compliance Review
- Security Review
- Legal Review

where appropriate.

Documentation

Exceptions shall:

- Be documented.
- Be approved.
- Include risk analysis.
- Include expiration dates.

9.25 Continuous Improvement

Processing governance activities shall be periodically reviewed to improve:

- Privacy Protection
- Security Protection
- Compliance Readiness
- Governance Maturity
- AI Governance
- Operational Effectiveness

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Major Technology Changes

The objective is to maintain a mature, auditable, accountable, secure, privacy-conscious, and enterprise-grade processing governance program supporting all information processing activities throughout the Cognera Health ecosystem.

10. HealScript™ Data Processing, Clinical Operations Governance, Documentation Governance, Care Coordination Governance, and Clinical Information Management

10.1 Purpose

Purpose Statement

The purpose of this section is to establish the governance, privacy, security, compliance, operational, clinical, artificial intelligence, information management, reporting, documentation, and lifecycle management requirements governing HealScript™.

HealScript™ serves as the primary practitioner, provider, care team, organizational management, documentation, reporting, analytics, operational intelligence, workflow management, and continuous care platform within the Cognera Health ecosystem.

Because HealScript™ processes highly sensitive healthcare information, including Protected Health Information (PHI), electronic Protected Health Information (ePHI), behavioral health information, mental health information, assessment information, treatment information, care coordination information, and AI-assisted outputs, enhanced governance and oversight are required.

This section establishes the framework through which HealScript™ data processing activities are authorized, controlled, monitored, audited, measured, and continuously improved.

10.2 Policy Statement

HealScript™ shall process information only for authorized healthcare, clinical, operational, reporting, compliance, security, customer-directed, and organizational purposes.

All HealScript™ processing activities shall support:

- Privacy Protection
- Security Protection
- Clinical Integrity
- Documentation Integrity

- Regulatory Compliance
- Data Quality
- AI Governance
- Operational Excellence
- Continuity of Care

All information processed through HealScript™ shall be governed according to:

- HIPAA
- HITECH
- Customer Requirements
- Contractual Requirements
- Privacy Policies
- Security Policies
- Data Retention Requirements
- AI Governance Requirements

10.3 HealScript™ Platform Governance Objectives

The HealScript™ Governance Program seeks to:

- **Support Care Delivery**
  - Enable authorized providers to deliver and document care.
- **Support Clinical Documentation**
  - Maintain accurate and reliable clinical records.
- **Support Measurement-Based Care**
  - Facilitate assessment administration, monitoring, and outcome measurement.
- **Support Care Coordination**
  - Enable communication and collaboration among authorized care teams.
- **Support Operational Intelligence**
  - Provide visibility into organizational performance and operations.
- **Support Compliance**
  - Support healthcare, privacy, security, and regulatory obligations.
- **Support Responsible AI**
  - Govern AI-assisted workflows and outputs.

10.4 HealScript™ Data Processing Scope

Information Categories

HealScript™ may process:

Clinical Documentation

- Clinical Notes
- Progress Notes
- SOAP Notes
- Session Notes
- Clinical Summaries

Treatment Information

- Treatment Plans
- Care Plans
- Recovery Plans

Assessment Information

- PHQ-9
- GAD-7
- OQ-45.2
- C-SSRS
- PCL-5
- ASRS
- AUDIT
- DAST
- WHO-5
- Custom Assessments

Care Coordination Information

- Referrals
- Follow-Up Activities
- Care Team Communications
- Coordination Records

Scheduling Information

- Appointments

- Calendars
- Session Information

Operational Information

- KPIs
- Utilization Metrics
- Productivity Metrics
- Operational Dashboards

AI Information

- AI Inputs
- AI Outputs
- AI Recommendations
- AI Summaries

10.5 HealScript™ Data Sources

Information may originate from:

Providers

- Documentation Activities
- Assessments
- Treatment Planning

Care Teams

- Coordination Activities
- Follow-Up Activities

Organizations

- Operational Activities
- Reporting Activities

HealConnect™

- Mood Data
- Journaling Data
- Assessment Data
- Engagement Data

Integrated Systems

- EHR Platforms
- Scheduling Platforms
- API Integrations
- Third-Party Systems

10.6 Clinical Documentation Governance

Policy Statement

Clinical documentation created, stored, modified, reviewed, transmitted, shared, archived, retained, or deleted within HealScript™ shall be governed as part of the clinical record.

Documentation Objectives

Support:

- Clinical Accuracy
- Continuity of Care
- Regulatory Compliance
- Documentation Integrity
- Auditability
- Accountability

Documentation Standards

Documentation should be:

- Accurate
- Complete
- Timely
- Relevant
- Legible
- Traceable
- Auditable

Documentation Controls

Examples include:

- Access Controls

- Audit Logging
- Version Management
- Change Tracking
- Monitoring
- Retention Controls

Documentation Reviews

Reviews may include:

- Provider Reviews
- Clinical Supervisor Reviews
- Quality Assurance Reviews
- Compliance Reviews

10.7 Assessment Governance

Policy Statement

Assessments administered, collected, processed, scored, reported, or retained within HealScript™ shall be governed through the Assessment Governance Program.

Assessment Objectives

Support:

- Screening
- Outcome Tracking
- Progress Monitoring
- Risk Identification
- Treatment Planning
- Quality Improvement

Assessment Processing Activities

Examples include:

- Administration
- Collection
- Scoring
- Trending
- Reporting

- Visualization
- AI-Assisted Analysis

Assessment Controls

Examples include:

- Validation Controls
- Access Controls
- Audit Logging
- Monitoring
- Retention Controls

Assessment Review Activities

Assessments may be reviewed by:

- Providers
- Care Teams
- Clinical Leadership
- Authorized Review Personnel

10.8 Treatment Planning Governance

Policy Statement

Treatment planning activities shall be governed to ensure quality, accountability, consistency, and continuity of care.

Treatment Planning Activities

Examples include:

- Treatment Plan Creation
- Treatment Plan Updates
- Goal Management
- Intervention Planning
- Progress Evaluation

Governance Requirements

Treatment planning shall support:

- Documentation Standards
- Provider Accountability
- Review Requirements
- Retention Requirements
- Auditability

10.9 Care Coordination Governance

Policy Statement

Care coordination activities shall support continuity of care while protecting privacy and confidentiality.

Care Coordination Activities

Examples include:

- Referrals
- Follow-Up Activities
- Care Team Communications
- Care Management Activities
- Cross-Disciplinary Collaboration

Governance Objectives

Support:

- Continuity of Care
- Communication
- Collaboration
- Accountability
- Documentation

Controls

Examples include:

- Access Controls
- Audit Logging
- Monitoring
- Disclosure Controls

- Retention Controls

10.10 Operational Intelligence Governance

Policy Statement

Operational intelligence capabilities shall be governed to ensure privacy, security, reliability, and appropriate use.

Operational Intelligence Activities

Examples include:

- KPI Monitoring
- Utilization Reporting
- Productivity Reporting
- Workflow Reporting
- Performance Monitoring
- Enterprise Reporting

Governance Requirements

Operational intelligence shall support:

- Data Minimization
- Privacy Controls
- Security Controls
- Monitoring
- Executive Oversight

10.11 Reporting Governance

Policy Statement

Reporting activities shall be governed to ensure appropriate access, distribution, quality, and accountability.

Report Categories

- Clinical Reports
- Assessment Reports

- Outcome Reports
- Operational Reports
- KPI Reports
- Executive Reports
- Compliance Reports

Report Controls

Examples include:

- Access Controls
- Distribution Controls
- Audit Logging
- Monitoring

10.12 HealScript™ Artificial Intelligence Governance

Policy Statement

AI-enabled capabilities within HealScript™ require enhanced governance.

AI Use Cases

Examples include:

- SOAP Draft Generation
- Session Summaries
- Documentation Assistance
- Reporting Assistance
- Workflow Assistance
- Trend Analysis

AI Governance Requirements

Examples include:

- Human Review
- Validation
- Monitoring
- Logging

- Risk Management
- Auditing

Clinical Restrictions

AI outputs shall not replace:

- Clinical Judgment
- Professional Judgment
- Regulatory Obligations
- Provider Accountability

10.13 Access Governance

Policy Statement

Access shall be limited according to:

- Role
- Function
- Need-to-Know
- Minimum Necessary

Authorized Roles

Examples include:

- Providers
- Care Teams
- Supervisors
- Administrators
- Compliance Personnel
- Security Personnel

Access Reviews

Reviews shall occur:

- Quarterly
- Following Role Changes
- Following Terminations

- Following Incidents

10.14 Audit Logging Governance

HealScript™ shall maintain logs supporting:

- Authentication Activities
- Record Access
- Record Modifications
- Documentation Activities
- Reporting Activities
- AI Activities
- Administrative Activities

Audit Objectives

Support:

- Accountability
- Investigations
- Compliance
- Security Monitoring

10.15 Information Sharing Governance

Information may be shared with:

- Covered Entities
- Authorized Providers
- Care Teams
- Authorized Customers
- Business Associates

where authorized and appropriate.

Sharing Controls

Examples include:

- Minimum Necessary

- Encryption
- Access Controls
- Logging
- Monitoring

10.16 Retention and Lifecycle Governance

Information processed within HealScript™ shall follow approved lifecycle management requirements.

Examples include:

- Clinical Records
- Assessments
- Communications
- AI Records
- Audit Records

Related Policies

See:

- Data Retention, Deletion, and Secure Disposal Policy
- Information Governance Program

10.17 Security Governance

HealScript™ shall support:

- Administrative Controls
- Technical Controls
- Operational Controls
- Monitoring Controls
- AI Security Controls
- Vendor Security Controls

Examples

- Encryption

- MFA
- RBAC
- Logging
- Monitoring
- Incident Response

10.18 Monitoring Program

Monitoring activities may include:

- Documentation Monitoring
- Assessment Monitoring
- Access Monitoring
- Security Monitoring
- AI Monitoring
- Compliance Monitoring

10.19 Auditing Program

Audits may include:

- Clinical Documentation Audits
- Privacy Audits
- Compliance Audits
- Security Audits
- AI Governance Audits
- Operational Audits

10.20 HealScript™ Metrics

Examples include:

- Documentation Completion Rates
- Assessment Completion Rates
- Treatment Plan Completion Rates
- Follow-Up Completion Rates

- AI Review Rates
- Access Review Completion Rates
- Audit Findings
- Privacy Incidents

10.21 Continuous Improvement

HealScript™ governance activities shall be reviewed periodically to improve:

- Privacy Protection
- Security Protection
- Documentation Quality
- Care Coordination
- Operational Efficiency
- Compliance Readiness
- AI Governance Maturity

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Major Platform Enhancements

The objective is to maintain a mature, secure, privacy-conscious, clinically responsible, auditable, and enterprise-grade platform governance program supporting all HealScript™ operations.

11. HealConnect™ Data Processing, Client Engagement Governance, Wellness Governance, Behavioral Health Engagement Governance, Consumer Health Data Governance, and Continuous Care Management

11.1 Purpose

Purpose Statement

The purpose of this section is to establish governance requirements governing the collection, processing, use, monitoring, sharing, retention, protection, and management of information processed through HealConnect™.

HealConnect™ serves as Cognera Health's engagement, communication, wellness, behavioral health support, assessment, journaling, recovery, and continuous care platform designed to facilitate meaningful interactions between individuals, providers, care teams, and organizations.

Unlike traditional healthcare platforms that primarily focus on episodic interactions, HealConnect™ is designed to support ongoing engagement between care interactions and therefore processes unique categories of information associated with wellness, mood, recovery, behavior, self-reporting, journaling, engagement, and continuity-of-care activities.

This section establishes the governance framework through which HealConnect™ supports privacy, security, compliance, consumer health data protections, responsible AI, and continuous care objectives.

11.2 Policy Statement

HealConnect™ shall process information only for authorized healthcare, behavioral health, wellness, engagement, communication, care coordination, recovery, educational, operational, compliance, security, and customer-directed purposes.

All HealConnect™ processing activities shall support:

- Privacy Protection
- Consumer Health Data Protection
- Security Protection

- Behavioral Health Data Protection
- Responsible AI Governance
- Transparency
- Accountability
- Continuity of Care
- Regulatory Compliance

Information processed through HealConnect™ shall be governed according to:

- Privacy Policies
- Consent Requirements
- Security Policies
- Data Retention Requirements
- Consumer Health Data Requirements
- AI Governance Requirements
- Customer Requirements

11.3 HealConnect™ Governance Objectives

The HealConnect™ Governance Program seeks to:

- **Support Engagement**
  - Enable meaningful engagement between individuals and care teams.
- **Support Wellness**
  - Support wellness, recovery, and self-management activities.
- **Support Behavioral Health**
  - Support behavioral health engagement and monitoring.
- **Support Continuous Care**
  - Facilitate care continuity between appointments and interventions.
- **Support Outcome Measurement**
  - Enable collection and monitoring of assessments and self-reported outcomes.
- **Support Responsible AI**
  - Ensure AI-enabled engagement activities remain governed and transparent.
- **Support Consumer Health Data Protection**
  - Apply enhanced protections to consumer health information.

11.4 HealConnect™ Information Categories

HealConnect™ may process:

- Personal Information
- Consumer Health Data
- Behavioral Health Information
- Wellness Information
- Mood Information
- Journaling Information
- Assessment Information
- Communications
- Voice Information
- Audio Information
- Crisis Information
- Engagement Information
- Recovery Information
- AI Inputs and Outputs

11.5 Personal Information Governance

Examples

Personal information may include:

- Name
- Username
- Contact Information
- Profile Information
- Account Information

Purpose

Used to support:

- Authentication
- Communications
- Account Management
- Engagement Activities

- Customer Support

Governance Requirements

Personal information shall support:

- Access Controls
- Encryption
- Monitoring
- Retention Controls
- Disposal Controls

11.6 Consumer Health Data Governance

Policy Statement

Consumer health data processed through HealConnect™ shall receive enhanced governance protections.

Examples

Consumer health data may include:

- Wellness Information
- Mood Information
- Recovery Information
- Behavioral Information
- Symptom Information
- Self-Reported Outcomes
- Health-Related Journaling

Governance Objectives

Support:

- Privacy Protection
- Transparency
- Accountability
- Regulatory Compliance
- Responsible Data Use

Controls

Examples include:

- Consent Controls
- Encryption
- Monitoring
- Audit Logging
- Retention Controls

11.7 Mood Tracking Governance

Policy Statement

Mood tracking activities shall be governed to support wellness, behavioral health engagement, continuity of care, and outcome measurement.

Examples

Mood information may include:

- Mood Scores
- Mood Trends
- Mood Journals
- Emotional Reflections
- Wellness Check-Ins

Governance Objectives

Support:

- Self-Awareness
- Engagement
- Outcome Monitoring
- Continuity of Care
- Provider Visibility

Controls

Examples include:

- Access Controls
- Monitoring
- Reporting Controls
- AI Governance Controls

11.8 Wellness Tracking Governance

Policy Statement

HealConnect™ may support wellness tracking activities.

Examples

- Wellness Check-Ins
- Lifestyle Activities
- Recovery Activities
- Goal Tracking
- Self-Care Activities
- Wellness Reflections

Governance Requirements

Wellness information shall support:

- **Privacy Controls**
- **Consumer Health Data Controls**
- **Monitoring**
- **Retention Controls**

11.9 Behavioral Health Engagement Governance

Policy Statement

Behavioral health engagement activities shall be governed to support continuity of care while protecting privacy and confidentiality.

Examples

- Recovery Activities
- Engagement Activities

- Reflection Activities
- Behavioral Health Journaling
- Follow-Up Activities

Governance Objectives

Support:

- Engagement
- Recovery
- Wellness
- Continuity of Care
- Outcome Measurement

Controls

Examples include:

- Access Controls
- Audit Logging
- Monitoring
- Retention Controls

11.10 Journaling Governance

Policy Statement

HealConnect™ may support structured and unstructured journaling activities.

Journaling Types

Examples include:

- Written Journals
- Guided Reflections
- Wellness Journals
- Recovery Journals
- Behavioral Health Journals
- Voice Journals

Governance Objectives

Support:

- Reflection
- Engagement
- Recovery
- Wellness
- Continuity of Care

Journaling Controls

Examples include:

- Encryption
- Access Controls
- Monitoring
- Retention Controls
- Secure Disposal

11.11 Voice Journaling Governance

Policy Statement

Voice journaling activities require enhanced governance due to the sensitivity of audio information.

Examples

- Voice Journals
- Voice Notes
- Voice Reflections
- Guided Audio Activities

Requirements

Examples include:

- Consent Controls
- Encryption
- Monitoring
- Retention Controls
- Disposal Controls

Regulatory Considerations

May include:

- HIPAA
- BIPA
- State Recording Laws
- Consumer Health Data Laws

11.12 Assessment Governance

Policy Statement

Assessments administered through HealConnect™ shall support outcome measurement, wellness monitoring, behavioral health activities, and continuity of care.

Examples

- PHQ-9
- GAD-7
- WHO-5
- OQ-45.2
- C-SSRS
- Custom Assessments

Governance Requirements

Examples include:

- Validation
- Access Controls
- Audit Logging
- Monitoring
- Reporting Controls

11.13 Messaging and Communications Governance

Policy Statement

HealConnect™ may support communications between individuals, providers, care teams, and organizations.

Examples

- Secure Messages
- Care Team Communications
- Follow-Up Messages
- Engagement Communications
- Wellness Notifications

Governance Requirements

Communications shall support:

- Encryption
- Access Controls
- Audit Logging
- Retention Controls
- Monitoring

11.14 Notification Governance

Policy Statement

Notifications shall support engagement while respecting privacy and consent preferences.

Examples

- Appointment Reminders
- Assessment Reminders
- Wellness Check-Ins
- Recovery Prompts
- Follow-Up Notifications

Governance Requirements

Examples include:

- Consent Controls
- Preference Management
- Opt-Out Support

- Monitoring

11.15 HealConnect™ Artificial Intelligence Governance

Policy Statement

HealConnect™ may utilize CogneraAI™ to support engagement, wellness, journaling, continuity of care, analytics, and workflow activities.

AI Use Cases

Examples include:

- Guided Reflections
- Wellness Prompts
- Engagement Suggestions
- Progress Summaries
- Trend Analysis
- Crisis Information
- Follow-Up Recommendations

Governance Requirements

Examples include:

- Human Oversight
- Validation
- Monitoring
- Transparency
- Explainability
- Audit Logging

Restrictions

AI outputs shall not replace:

- Clinical Judgment
- Professional Judgment
- Provider Accountability

11.16 Engagement Analytics Governance

Policy Statement

Engagement analytics shall be governed to support visibility into participation, adherence, engagement, and wellness activities.

Examples

- Engagement Trends
- Participation Metrics
- Assessment Completion
- Follow-Up Completion
- Wellness Activity Participation

Controls

Examples include:

- Data Minimization
- Privacy Controls
- Access Controls
- Reporting Controls

11.17 Information Sharing Governance

Information may be shared with:

- Authorized Providers
- Authorized Care Teams
- Authorized Organizations
- Covered Entities
- Business Associates

where authorized and appropriate.

Controls

Examples include:

- Minimum Necessary
- Access Controls

- Encryption
- Monitoring
- Audit Logging

11.18 Retention and Lifecycle Governance

Information processed through HealConnect™ shall follow approved lifecycle requirements.

Examples include:

- Journals
- Assessments
- Communications
- Voice Records
- Consumer Health Data
- AI Records

Related Policies

- Data Retention Policy
- Information Governance Program
- Voice Governance Program

11.19 Security Governance

HealConnect™ shall support:

- Administrative Controls
- Technical Controls
- Operational Controls
- Consumer Health Data Controls
- AI Security Controls
- Voice Security Controls

Examples

- Encryption
- MFA

- RBAC
- Logging
- Monitoring
- Incident Response

11.20 Monitoring Program

Monitoring activities may include:

- Engagement Monitoring
- Assessment Monitoring
- Voice Monitoring
- Security Monitoring
- AI Monitoring
- Privacy Monitoring

Objectives

Support:

- Privacy Protection
- Security Protection
- Quality Improvement
- Compliance Readiness

11.21 Auditing Program

Audits may include:

Privacy Audits

- Consumer Health Data Audits
- Security Audits
- AI Governance Audits
- Voice Governance Audits
- Operational Audits

11.22 HealConnect™ Metrics

Examples include:

- Engagement Rates
- Assessment Completion Rates
- Follow-Up Completion Rates
- Wellness Participation Rates
- AI Review Rates
- Privacy Findings
- Security Findings
- Consumer Health Data Findings

11.23 Continuous Improvement

HealConnect™ governance activities shall be reviewed periodically to improve:

- Privacy Protection
- Security Protection
- Consumer Health Data Protection
- Engagement
- Wellness Outcomes
- Recovery Support
- Compliance Readiness
- AI Governance Maturity

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Major Platform Enhancements

The objective is to maintain a mature, secure, privacy-conscious, consumer-focused, auditable, and enterprise-grade engagement governance program supporting all HealConnect™ operations.

12. CogneraAI™ Data Processing, Artificial Intelligence Operations, AI Governance, Model Governance, AI Risk Management, and Responsible AI Program

12.1 Purpose

Purpose Statement

The purpose of this section is to establish the governance, oversight, accountability, validation, monitoring, security, privacy, compliance, risk management, transparency, explainability, and operational requirements governing CogneraAI™ and all artificial intelligence capabilities deployed within the Cognera Health™ ecosystem.

Artificial Intelligence represents one of the most significant opportunities and risks within modern healthcare technology.

Cognera Health recognizes that AI systems may influence:

- Clinical Workflows
- Documentation Activities
- Operational Decision-Making
- Engagement Activities
- Reporting Activities
- Care Coordination Activities
- Administrative Activities
- Information Processing Activities

Accordingly, AI systems require governance controls beyond traditional privacy and security requirements.

This section establishes the enterprise AI governance framework designed to ensure that AI technologies remain:

- Responsible
- Transparent
- Explainable
- Auditable
- Accountable
- Privacy-Conscious

- Secure
- Human-Governed

12.2 Policy Statement

CogneraAI™ shall operate within a comprehensive Artificial Intelligence Governance Framework designed to ensure that AI-enabled processing activities remain lawful, ethical, secure, privacy-conscious, transparent, explainable, auditable, and appropriately governed.

AI technologies shall support and augment human decision-making.

AI technologies shall not replace:

- Clinical Judgment
- Professional Judgment
- Human Accountability
- Regulatory Responsibilities
- Organizational Governance

Final responsibility for decisions remains with:

- Providers
- Care Teams
- Organizations
- Authorized Users
- Organizational Leadership

12.3 AI Governance Objectives

The AI Governance Program seeks to:

- **Improve Documentation**
  - Reduce administrative burden while maintaining quality and oversight.
- **Improve Operational Intelligence**
  - Provide enhanced visibility into operations.
- **Improve Engagement**
  - Support wellness, recovery, and engagement activities.
- **Improve Analytics**

    - Support trend identification and reporting.
- **Support Responsible Innovation**
    - Enable safe and ethical AI adoption.
- **Reduce Risk**
    - Reduce:
        - Privacy Risk
        - Security Risk
        - AI Risk
        - Clinical Risk
        - Regulatory Risk
        - Operational Risk
        - Reputational Risk
- **Maintain Trust**
    - Maintain confidence in AI-enabled capabilities.

12.4 AI Governance Principles

Human-in-the-Loop

Human oversight shall remain central to AI-enabled activities.

Humans shall:

- Review Outputs
- Validate Outputs
- Approve Outputs
- Reject Outputs
- Override Outputs
- Escalate Concerns

AI shall support—not replace—human decision-making.

Transparency

Users should understand:

- When AI is used.
- Why AI is used.
- What AI is doing.
- What limitations exist.

Explainability
AI outputs should be understandable and explainable where reasonably feasible.

Accountability

- Responsibility remains with humans.
- AI systems do not assume accountability.

Fairness

AI systems shall be monitored for:

- Bias
- Disparate Outcomes
- Fairness Concerns
- Unintended Consequences

Privacy Protection

AI systems shall support:

- Privacy Requirements
- Data Minimization
- Consent Requirements
- Information Governance Requirements

Security Protection

AI systems shall support:

- Encryption
- Access Controls
- Monitoring
- Logging
- Security Reviews

12.5 AI Governance Structure

AI governance shall be supported through:

- **Executive Leadership**
  - Strategic oversight.

- **Privacy Officer**
  - Privacy oversight.
- **Compliance Officer**
  - Regulatory oversight.
- **CISO**
  - Security oversight.
- **Legal Counsel**
  - Legal review.
- **Data Governance Steering Committee**
  - Governance oversight.
- **AI Governance Owner**
  - Operational ownership.
- **Product Leadership**
  - AI feature ownership.
- **Engineering Leadership**
  - Technical implementation ownership.

12.6 AI Inventory Program

Policy Statement

Cognera Health shall maintain a comprehensive inventory of AI systems.

Inventory Contents

Examples include:

- AI System Name
- Business Purpose
- Owner
- Vendor
- Inputs
- Outputs
- Risk Classification
- Validation Status
- Deployment Status
- Retirement Status

Inventory Reviews

Inventories shall be reviewed periodically.

12.7 AI Risk Classification Framework

All AI systems shall be assigned a risk classification.

Low Risk AI

Examples:

- Administrative Automation
- Non-Sensitive Reporting
- Internal Productivity Features

Moderate Risk AI

Examples:

- Workflow Assistance
- Reporting Assistance
- Operational Recommendations

High Risk AI

Examples:

- Clinical Documentation Assistance
- Behavioral Health Recommendations
- Care Coordination Intelligence
- Engagement Intelligence

Critical Risk AI

Examples:

- Large-Scale Clinical Influence
- High-Impact Predictive Models
- Regulatory-Sensitive Processing

Governance Requirements

Higher risk classifications require:

- Additional Validation

- Additional Monitoring
- Additional Oversight
- Additional Approval

12.8 AI Approval Program

Policy Statement

AI capabilities shall not be deployed into production without appropriate review and approval.

Approval Activities

Examples include:

- Privacy Review
- Security Review
- Compliance Review
- AI Governance Review
- Legal Review
- Risk Review

Approval Authorities

Approvals may require:

- Privacy Officer
- Compliance Officer
- CISO
- Steering Committee

12.9 AI Data Processing Governance

AI Inputs

Examples include:

- Clinical Documentation
- Assessments
- Treatment Plans
- Care Plans

- Journals
- Voice Transcriptions
- Messages
- Operational Data

AI Outputs

Examples include:

- Summaries
- Recommendations
- Draft Documentation
- Insights
- Alerts
- Reports
- Trend Analysis

Processing Requirements

AI processing shall support:

- Privacy Controls
- Security Controls
- Human Oversight
- Logging
- Monitoring

12.10 Human-in-the-Loop Governance

Policy Statement

Human review is mandatory for AI-enabled activities involving healthcare information, behavioral health information, documentation, recommendations, and decision support.

Human Review Activities

Examples include:

- Output Review
- Output Validation

- Output Approval
- Output Modification
- Output Rejection
- Escalation

Clinical Activities

AI-generated documentation or recommendations shall not be relied upon without appropriate review.

12.11 AI Validation Program

Policy Statement

AI systems shall undergo validation before deployment and periodically thereafter.

Validation Objectives

Evaluate:

- Accuracy
- Reliability
- Consistency
- Performance
- Safety
- Fairness
- Explainability

Validation Activities

Examples include:

- Functional Testing
- Output Review
- Clinical Review
- Privacy Review
- Security Review
- Bias Review

Validation Documentation

Examples include:

- Validation Reports
- Approval Records
- Monitoring Records

12.12 AI Monitoring Program

Policy Statement

AI systems shall undergo ongoing monitoring.

Monitoring Objectives

Monitor:

- Accuracy
- Reliability
- Performance
- Fairness
- Security
- Privacy
- Drift

Monitoring Activities

Examples include:

- Output Monitoring
- Trend Monitoring
- Drift Monitoring
- Bias Monitoring
- Error Monitoring

12.13 Bias Management Program

Policy Statement

Cognera Health recognizes that AI systems may produce biased outcomes.

Bias Sources

Examples include:

- Training Data Bias
- Sampling Bias
- Representation Bias
- Labeling Bias
- Model Bias
- Deployment Bias

Mitigation Activities

Examples include:

- Validation
- Monitoring
- Human Review
- Governance Reviews
- Corrective Actions

12.14 Explainability and Transparency Program

Policy Statement

Cognera Health shall seek to improve transparency and explainability associated with AI-enabled activities.

Objectives

Support:

- User Understanding
- Trust
- Accountability
- Regulatory Readiness

Transparency Activities

Examples include:

- User Notices
- AI Disclosures
- Documentation

- Governance Reviews

12.15 AI Security Program

Policy Statement

AI systems require enhanced security governance.

Threat Categories

Examples include:

- Prompt Injection
- Model Manipulation
- Data Leakage
- Unauthorized Access
- Output Abuse
- Training Data Exposure

Security Controls

Examples include:

- Encryption
- MFA
- RBAC
- Logging
- Monitoring
- Vulnerability Management

12.16 AI Vendor Governance

Policy Statement

Third-party AI providers shall undergo enhanced governance review.

Vendor Review Activities

Examples include:

- Privacy Reviews
- Security Reviews

- Contract Reviews
- Risk Assessments
- AI Governance Reviews

Requirements

Vendors shall support:

- Privacy Protection
- Security Protection
- Transparency
- Auditability

12.17 AI Incident Management

Examples

- Hallucinations
- Inaccurate Outputs
- Bias Findings
- Security Incidents
- Privacy Incidents
- Unauthorized Processing

Response Activities

Examples include:

- Investigation
- Containment
- Remediation
- Monitoring
- Governance Review

12.18 AI Audit Program

Policy Statement

AI activities shall be auditable.

Audit Areas

Examples include:

- Inputs
- Outputs
- Validation
- Monitoring
- Human Reviews
- Overrides
- Incidents

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Risk Exposure
- Control Effectiveness

12.19 AI Metrics and Reporting

Examples include:

- Validation Rates
- Human Review Rates
- Override Rates
- Bias Findings
- Drift Findings
- Incident Volume
- Adoption Rates
- Audit Findings

Reporting Recipients

Examples include:

- Privacy Officer
- Compliance Officer
- CISO

- Steering Committee
- Executive Leadership

12.20 AI Lifecycle Management

AI systems shall be governed throughout:

- Design
- Development
- Testing
- Validation
- Deployment
- Monitoring
- Retirement

Governance Reviews

Each lifecycle stage may require:

- Privacy Review
- Security Review
- Compliance Review
- Risk Review
- AI Governance Review

12.21 AI Retirement Program

Policy Statement

Retired AI systems shall undergo controlled decommissioning.

Activities

Examples include:

- Access Removal
- Inventory Updates
- Monitoring Termination
- Documentation Preservation

- Secure Disposal

12.22 Continuous Improvement

The AI Governance Program shall be periodically reviewed to improve:

- Transparency
- Explainability
- Accountability
- Fairness
- Privacy Protection
- Security Protection
- Governance Maturity
- Regulatory Readiness

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Significant AI Changes
- Following Regulatory Changes

The objective is to maintain a mature, trustworthy, privacy-conscious, secure, transparent, explainable, auditable, and enterprise-grade Artificial Intelligence Governance Program supporting all AI-enabled activities throughout the Cognera Health ecosystem.

13. Voice-to-Text, Audio Processing, Recording Governance, Speech Processing Controls, Biometric Information Governance, and Voice Data Protection Program

13.1 Purpose

Purpose Statement

The purpose of this section is to establish the governance, privacy, security, compliance, consent, retention, monitoring, auditing, and lifecycle management requirements governing voice recordings, audio files, speech processing, voice-to-text technologies, audio analytics, transcriptions, telehealth recordings, voice journals, voice notes, dictation activities, and related voice-enabled services within the Cognera Health™ ecosystem.

Voice and audio information frequently contain highly sensitive information that may reveal:

- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)
- Behavioral Health Information
- Mental Health Information
- Consumer Health Data
- Crisis Information
- Wellness Information
- Treatment Information
- Personal Information
- Sensitive Personal Information

Voice information may also contain emotional, contextual, behavioral, and clinical indicators that are not always present in written information.

Accordingly, voice and audio information require enhanced governance, oversight, accountability, consent management, monitoring, security, and privacy protections.

13.2 Policy Statement

Cognera Health shall implement enhanced governance requirements governing all voice, audio, recording, transcription, speech-processing, and voice-to-text activities.

Voice processing activities shall support:

- Privacy Protection
- Security Protection
- Consent Governance
- Transparency
- Accountability
- Regulatory Compliance
- Responsible AI Governance

- Consumer Health Data Protection

Voice information shall be collected, processed, retained, shared, disclosed, monitored, archived, deleted, and disposed of only according to approved governance requirements.

13.3 Voice Governance Objectives

The Voice Governance Program seeks to:

Protect Privacy
Protect individuals from unauthorized use or disclosure of voice information.

Support Regulatory Compliance
Support obligations arising from:

- HIPAA
- HITECH
- BIPA
- State Recording Laws
- Consumer Health Data Laws
- Privacy Laws

Support Accessibility
Provide voice-enabled capabilities supporting accessibility and usability.

Support Documentation
Enable efficient and accurate documentation workflows.

Support Responsible AI
Ensure AI-enabled speech processing remains governed.

Reduce Risk
Reduce:

- Privacy Risk
- Security Risk
- Regulatory Risk
- AI Risk
- Operational Risk

13.4 Voice Processing Scope

This section applies to:

- Voice Journals
- Voice Notes

- Clinical Dictation
- Telehealth Audio
- Session Recordings
- Voice-to-Text Activities
- Audio Analytics
- Speech Recognition
- AI Speech Processing
- Voice Metadata
- Audio Archives
- Audio Backups
- Voice-Derived Outputs

13.5 Voice Data Classification

Policy Statement

Voice and audio information shall generally be classified as Restricted Information unless otherwise approved.

Risk Factors

Voice information may reveal:

- Identity
- Health Status
- Mental Health Conditions
- Emotional State
- Treatment Information
- Recovery Activities
- Behavioral Indicators

Classification Requirements

Voice information shall support:

- **Enhanced Access Controls**
- **Enhanced Monitoring**
- **Enhanced Retention Controls**
- **Enhanced Disposal Controls**

13.6 Voice Collection Governance

Policy Statement

Voice information shall be collected only when:

- Authorized
- Necessary
- Documented
- Transparent
- Appropriate

Authorized Collection Activities

Examples include:

- Voice Journaling
- Clinical Dictation
- Telehealth Activities
- Wellness Activities
- Recovery Activities
- Care Coordination Activities

Collection Controls

Examples include:

- Consent Verification
- Privacy Notices
- Access Controls
- Monitoring
- Audit Logging

13.7 Recording Governance

Policy Statement

Recording activities require enhanced governance due to legal, privacy, and regulatory implications.

Recording Types

Examples include:

- Audio Recording
- Telehealth Recording
- Session Recording
- Clinical Recording
- Voice Journaling
- Wellness Recording

Governance Requirements

Recording activities shall support:

- Notice
- Consent
- Documentation
- Monitoring
- Retention Controls
- Deletion Controls

Recording Restrictions

Unauthorized recording is prohibited.

13.8 Consent Governance for Voice Activities

Policy Statement

Voice processing activities may require consent depending on applicable requirements.

Consent Triggers

Consent may be required before:

- Recording
- Voice Analysis
- Voice-to-Text Processing
- AI Voice Processing
- Telehealth Recording
- Session Recording

Consent Methods

Examples include:

- Electronic Consent

- Written Consent
- Clickwrap Consent
- Point-of-Use Consent
- HIPAA Authorization

Documentation Requirements

Consent records shall be:

- Retained
- Auditable
- Verifiable

13.9 Voice-to-Text Governance

Policy Statement

Voice-to-text technologies shall be used only for authorized purposes.

Examples

- Documentation Assistance
- Clinical Dictation
- Journaling Support
- Accessibility Support
- Workflow Assistance

Processing Controls

Examples include:

- Encryption
- Logging
- Monitoring
- Validation
- Access Controls

Quality Controls

Examples include:

- Transcription Accuracy Reviews

- Human Review
- Error Correction
- Validation Activities

13.10 Telehealth Audio Governance

Policy Statement

Telehealth recordings require enhanced governance and oversight.

Examples

- Audio Sessions
- Video Sessions
- Session Recordings
- Session Transcriptions
- Session Summaries

Controls

Examples include:

- Consent
- Encryption
- Access Controls
- Monitoring
- Retention Controls
- Secure Disposal

13.11 Voice Journaling Governance

Policy Statement

Voice journaling activities shall support privacy, wellness, behavioral health engagement, and continuity-of-care objectives.

Examples

- Personal Reflections
- Wellness Journals
- Recovery Journals

- Behavioral Health Journals
- Guided Reflections

Governance Controls

Examples include:

- Consent
- Encryption
- Access Controls
- Monitoring
- Retention Controls

13.12 Voice Artificial Intelligence Governance

Policy Statement

AI-enabled voice processing requires enhanced governance.

Examples

- Speech Recognition
- Voice Summarization
- Documentation Generation
- Audio Analytics
- Voice Classification

Governance Requirements

Examples include:

- Human Review
- Validation
- Monitoring
- Logging
- Risk Reviews
- AI Governance Reviews

Restrictions

Voice AI outputs shall not replace:

- Clinical Judgment

- Professional Judgment
- Human Accountability

13.13 Voice Metadata Governance

Examples

Voice metadata may include:

- Recording Time
- Recording Date
- Duration
- Device Information
- Session Information
- Processing Information

Governance Requirements
Metadata shall be governed according to its sensitivity and associated risks.

13.14 Biometric Information Governance

Policy Statement

Cognera Health does not intentionally collect, store, sell, lease, trade, or otherwise monetize biometric identifiers unless specifically authorized, legally permissible, and approved through governance processes.

Potential Biometric Information

Examples may include:

- Voiceprints
- Voice Biometrics
- Biometric Templates
- Biometric Identifiers

Governance Requirements

Examples include:

- Notice Requirements
- Consent Requirements

- Retention Controls
- Disposal Controls
- Enhanced Security Controls

13.15 BIPA Compliance Governance

Purpose

Support governance obligations associated with biometric information privacy requirements.

Governance Areas

Examples include:

- Notice
- Consent
- Retention
- Destruction
- Access Controls
- Auditability

Restrictions

Biometric information shall not be:

- Sold
- Leased
- Traded
- Monetized

without lawful authority and governance approval.

13.16 Voice Security Controls

Voice information shall support enhanced protections.

Administrative Controls

Examples include:

- Policies

- Training
- Governance Reviews
- Risk Assessments

Technical Controls

Examples include:

- AES-256 Encryption
- TLS
- MFA
- RBAC
- Logging
- Monitoring

Operational Controls

Examples include:

- Monitoring
- Incident Response
- Auditing
- Disposal Verification

13.17 Voice Retention Governance

Policy Statement

Voice information shall be retained only as long as necessary.

Examples

- **Raw Audio**
  - May be deleted following successful transcription and validation unless retention is required.
- **Transcriptions**
  - May follow clinical record retention requirements.
- **Metadata**
  - May follow approved retention schedules.
- **AI Voice Records**
  - May follow AI governance retention requirements.

Related Policy

See: **Data Retention, Deletion, and Secure Disposal Policy**

13.18 Voice Disposal Governance

Policy Statement

Voice information shall be securely disposed of when no longer required.

Disposal Activities

Examples include:

- Secure Deletion
- Cryptographic Erasure
- Media Sanitization
- Secure Cloud Destruction
- Key Destruction

Objectives

Prevent:

- Unauthorized Recovery
- Reconstruction
- Disclosure

13.19 Voice Risk Management

Risk Categories

Examples include:

- Privacy Risks
- Security Risks
- Regulatory Risks
- AI Risks
- Accuracy Risks
- Recording Risks
- Biometric Risks

Mitigation Activities

Examples include:

- Monitoring
- Auditing
- Validation
- Reviews
- Corrective Actions

13.20 Voice Monitoring Program

Monitoring activities may include:

- Access Monitoring
- Consent Monitoring
- Recording Monitoring
- Security Monitoring
- AI Monitoring
- Retention Monitoring

Objectives

Identify:

- Unauthorized Access
- Unauthorized Recording
- Consent Failures
- Processing Failures
- Governance Gaps

13.21 Voice Auditing Program

Audits may include:

- Privacy Audits
- Security Audits
- Consent Audits
- AI Audits

- Retention Audits
- Voice Governance Audits

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Security Controls
- Consent Controls
- Risk Exposure

13.22 Voice Metrics

Examples include:

- Voice Consent Compliance
- Transcription Accuracy
- Voice Audit Findings
- Voice Incidents
- Voice Retention Compliance
- Voice AI Findings
- Unauthorized Recording Findings

13.23 Continuous Improvement

Voice governance activities shall be periodically reviewed to improve:

- Privacy Protection
- Security Protection
- Accessibility
- Accuracy
- Transparency
- Compliance Readiness
- AI Governance
- Risk Management

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Technology Changes

The objective is to maintain a mature, auditable, privacy-conscious, secure, transparent, and enterprise-grade Voice Governance Program supporting all speech-processing activities throughout the Cognera Health ecosystem.

14. Consent Management Program, Authorization Governance, Consent Lifecycle Management, and Individual Choice Framework

14.1 Purpose

Purpose Statement

The purpose of this section is to establish a comprehensive enterprise Consent Management Program governing the collection, documentation, validation, storage, use, modification, monitoring, withdrawal, retention, auditing, and governance of consents, authorizations, acknowledgements, permissions, agreements, and individual choices associated with information processing activities throughout the Cognera Health™ ecosystem.

Consent serves as a critical mechanism supporting transparency, individual autonomy, privacy rights, trust, accountability, and regulatory compliance.

Because consent obligations vary across healthcare regulations, privacy laws, consumer protection laws, consumer health data laws, artificial intelligence governance requirements, telehealth requirements, voice processing requirements, and contractual obligations, Cognera Health shall maintain a centralized governance framework governing all consent-related activities.

14.2 Policy Statement

Cognera Health shall maintain a formal Consent Management Program designed to ensure that individuals are provided appropriate notice, transparency, choice, and control regarding information processing activities where consent, authorization, acknowledgement, acceptance, or affirmative agreement is required.

The Consent Management Program shall support:

- HIPAA Requirements
- HITECH Requirements
- GDPR Requirements
- UK GDPR Requirements
- CCPA / CPRA Requirements
- Consumer Health Data Requirements
- Telehealth Requirements
- AI Governance Requirements
- Voice Processing Requirements
- Customer Requirements

All consent activities shall be:

- Documented
- Verifiable
- Auditable
- Traceable
- Governed
- Monitored

14.3 Consent Governance Objectives

The Consent Management Program seeks to:

- **Support Individual Choice**
  - Allow individuals to make informed decisions.
- **Promote Transparency**
  - Ensure individuals understand information practices.
- **Support Compliance**
  - Support applicable legal and regulatory requirements.
- **Support Responsible AI**

    - Provide transparency regarding AI-enabled processing.
- **Support Voice Processing Governance**
    - Ensure recording and voice activities are appropriately governed.
- **Reduce Regulatory Risk**
    - Reduce consent-related compliance risks.
- **Maintain Trust**
    - Promote confidence in information handling practices.

14.4 Consent Governance Principles

All consent activities shall support the following principles.

Transparency

Individuals should understand:

- What they are agreeing to.
- Why information is being collected.
- How information will be used.
- How information may be shared.
- How information will be retained.

Informed Choice
Individuals should be provided sufficient information to make informed decisions.

Voluntary Participation
Where consent is required, consent should be freely provided.

Specificity
Consent should be associated with specific activities.

Documentation
Consent activities shall be documented and auditable.

Revocability
Where legally permissible, individuals may withdraw consent.

Accountability
Consent activities shall be governed and monitored.

14.5 Consent Governance Framework

The Consent Management Program consists of:

- HIPAA Authorization Governance
- Privacy Consent Governance
- AI Consent Governance
- Voice Consent Governance
- Recording Consent Governance
- Telehealth Consent Governance
- Marketing Consent Governance
- Research Consent Governance
- Consumer Health Data Consent Governance
- Consent Verification Governance
- Consent Withdrawal Governance
- Consent Auditing Governance

14.6 Consent Categories

HIPAA Authorization
Authorization associated with uses or disclosures of PHI where authorization is required.

Privacy Consent
Consent associated with privacy-related processing activities.

Artificial Intelligence Consent
Consent associated with AI-enabled processing where required.

Voice Consent
Consent associated with recording, transcription, voice processing, or speech-processing activities.

Recording Consent
Consent associated with audio or video recording activities.

Telehealth Consent
Consent associated with telehealth participation and related services.

Marketing Consent
Consent associated with marketing communications.

Research Consent
Consent associated with research activities.

Consumer Health Data Consent
Consent associated with processing consumer health information where required.

14.7 HIPAA Authorization Governance

Policy Statement

Certain uses and disclosures of PHI may require HIPAA Authorization.

Examples

HIPAA Authorizations may be required for:

- Marketing Activities
- Research Activities
- Non-TPO Activities
- Certain AI Activities
- Certain Third-Party Disclosures

Authorization Requirements

Authorizations should identify:

- Information Involved
- Purpose
- Recipient
- Expiration
- Revocation Rights
- Individual Acknowledgement

Governance Requirements

HIPAA Authorizations shall support:

- Verification
- Documentation
- Retention
- Auditing

14.8 Artificial Intelligence Consent Governance

Policy Statement

Cognera Health supports transparency regarding AI-enabled processing.

Examples

AI-enabled activities may include:

- Documentation Assistance
- Summarization
- Analytics
- Recommendations
- Voice Processing
- Workflow Assistance

Objectives

Support:

- Transparency
- User Awareness
- Trust
- Responsible AI

Consent Activities

Individuals may receive information regarding:

- AI Usage
- AI Limitations
- Human Oversight
- AI Governance Controls

14.9 Voice Consent Governance

Policy Statement

Voice processing activities may require consent depending upon applicable requirements.

Examples

- Voice Journals
- Voice Notes
- Recording Activities
- Voice-to-Text
- Telehealth Recording
- AI Voice Processing

Governance Requirements

Voice consent activities shall support:

- Documentation
- Auditability
- Verification
- Retention

14.10 Recording Consent Governance

Policy Statement

Recording activities require enhanced governance.

Recording Activities

Examples include:

- Audio Recording
- Video Recording
- Session Recording
- Clinical Recording
- Telehealth Recording

Governance Requirements

Recording activities shall support:

- Notice
- Consent
- Documentation

- Monitoring
- Retention Controls

14.11 Telehealth Consent Governance

Policy Statement

Telehealth participation may require consent and authorization.

Telehealth Governance Areas

Examples include:

- Identity Verification
- Telehealth Participation
- Recording Authorization
- Communication Authorization
- Documentation Authorization

Documentation Requirements

Telehealth consent records shall be retained according to approved retention schedules.

14.12 Consumer Health Data Consent Governance

Policy Statement

Consumer health data may require additional consent controls.

Examples

- Mood Tracking
- Wellness Tracking
- Recovery Activities
- Symptom Tracking
- Consumer Health Data Sharing

Governance Requirements

Examples include:

- Transparency

- Notice
- Consent
- Withdrawal Mechanisms
- Auditing

14.13 Marketing Consent Governance

Policy Statement

Marketing activities shall support applicable consent requirements.

Examples

- Product Announcements
- Promotional Communications
- Event Invitations
- Educational Communications

Consent Controls

Examples include:

- Opt-In
- Opt-Out
- Preference Management
- Consent Tracking

14.14 Research Consent Governance

Policy Statement

Research-related processing activities shall support applicable consent and authorization requirements.

Examples

- Research Studies
- Product Research
- AI Research
- Analytics Research

Governance Requirements

Examples include:

- Authorization
- Consent
- Ethics Review
- Documentation
- Monitoring

14.15 Clickwrap and Electronic Consent Governance

Policy Statement

Cognera Health may utilize electronic consent mechanisms.

Examples

- EULA Acceptance
- Privacy Policy Acceptance
- Terms Acceptance
- AI Consent
- Voice Consent
- Telehealth Consent

Requirements

Electronic consent shall:

- Capture Affirmative Action
- Record Acceptance
- Support Auditability
- Support Verification

14.16 Point-of-Use Consent Governance

Policy Statement

Certain activities may require consent immediately before the activity occurs.

Examples

- Recording
- AI Processing
- Voice Processing
- Telehealth Recording
- Sensitive Data Collection

Governance Requirements

Point-of-use consent shall be:

- Timely
- Relevant
- Contextual
- Auditable

14.17 Consent Verification Program

Policy Statement

Cognera Health shall verify consent where required.

Verification Activities

Examples include:

- Identity Verification
- Authorization Validation
- Consent Validation
- Record Verification

Restrictions

Activities requiring consent shall not proceed if consent cannot be verified.

14.18 Consent Withdrawal Program

Policy Statement

Where legally permissible, individuals may withdraw consent.

Withdrawal Methods

Examples include:

- Privacy Office Requests
- Customer Administrator Requests
- Application Controls
- Written Requests

Effects of Withdrawal

Withdrawal may:

- Limit Functionality
- Restrict Features
- Restrict Participation
- Restrict Processing Activities

Activities Not Affected

Withdrawal generally does not affect:

- Prior Lawful Processing
- Legal Obligations
- Security Obligations
- Retention Obligations

14.19 Consent Documentation Requirements

Consent records may include:

- Individual Identifier
- Consent Type
- Date
- Method
- Scope
- Version Accepted
- Withdrawal Status
- Verification Information

Retention

Consent records shall be retained according to approved retention schedules.

14.20 Consent Monitoring Program

Monitoring activities may include:

- Consent Capture
- Consent Verification
- Consent Withdrawal
- Recording Consent
- Voice Consent
- AI Consent

Objectives

Identify:

- Missing Consents
- Invalid Consents
- Expired Consents
- Governance Gaps

14.21 Consent Auditing Program

Audits may include:

- HIPAA Authorization Audits
- Voice Consent Audits
- AI Consent Audits
- Telehealth Consent Audits
- Consumer Health Data Consent Audits

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Documentation Quality
- Control Effectiveness

14.22 Consent Metrics

Examples include:

- Consent Capture Rate
- Verification Rate
- Withdrawal Rate
- Consent Audit Findings
- Voice Consent Compliance
- AI Consent Compliance
- Telehealth Consent Compliance

14.23 Roles and Responsibilities

Privacy Officer

Responsible for:

- Consent Governance
- Consent Reviews
- Consent Escalations

Compliance Officer

Responsible for:

- Compliance Monitoring
- Audit Oversight

Legal Counsel

Responsible for:

- Legal Interpretation
- Regulatory Guidance

Data Governance Steering Committee

Responsible for:

- Governance Oversight

- Policy Approval

14.24 Continuous Improvement

The Consent Management Program shall be periodically reviewed to improve:

- Transparency
- User Understanding
- Compliance
- Privacy Protection
- Governance Maturity
- Regulatory Readiness

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Major Technology Changes

The objective is to maintain a mature, transparent, auditable, compliant, and enterprise-grade Consent Management Program supporting all information processing activities throughout the Cognera Health ecosystem.

15. Information Sharing, Disclosures, Data Transfers, Third-Party Sharing, Disclosure Governance, and Information Exchange Management

15.1 Purpose

Purpose Statement

The purpose of this section is to establish enterprise governance requirements governing the sharing, disclosure, transfer, transmission, publication, release, exchange, export, exposure, provision, distribution, and communication of information by Cognera Health™.

Information sharing is a necessary component of healthcare delivery, care coordination, customer operations, vendor management, analytics, reporting, compliance activities, security operations, and organizational governance. However, inappropriate disclosures may create significant privacy, security, legal, regulatory, operational, clinical, and reputational risks.

This section establishes the governance framework through which information sharing activities shall be authorized, controlled, monitored, documented, audited, and continuously improved.

The organization recognizes that disclosure governance is a critical privacy control requiring heightened oversight, accountability, transparency, and risk management.

15.2 Policy Statement

Cognera Health shall limit the sharing, disclosure, transfer, exchange, transmission, publication, export, exposure, release, or provision of information to circumstances that are:

- Authorized
- Necessary
- Appropriate
- Lawful
- Contractually Permitted
- Operationally Justified
- Properly Documented

All information sharing activities shall support:

- Privacy Protection
- Security Protection
- Regulatory Compliance
- Accountability
- Transparency
- Data Minimization
- Risk Management

Information shall not be disclosed, shared, or transferred without an appropriate legal basis, contractual basis, customer authorization, regulatory authorization, governance

approval, or other lawful authority.

15.3 Information Sharing Governance Objectives

The Information Sharing Governance Program seeks to:

Support Care Delivery
Enable lawful and appropriate sharing supporting healthcare activities.

Support Continuity of Care
Enable coordination among authorized providers and care teams.

Support Customer Requirements
Support customer-authorized information exchange.

Support Regulatory Compliance
Support lawful disclosure activities.

Reduce Privacy Risk
Reduce unauthorized disclosure risks.

Reduce Security Risk
Reduce unauthorized access and exposure risks.

Improve Accountability
nsure sharing activities are documented and auditable.

15.4 Information Sharing Principles

All sharing activities shall support:

- Minimum Necessary
- Purpose Limitation
- Authorization
- Accountability
- Transparency
- Security
- Documentation
- Auditability
- Risk Management

15.5 Minimum Necessary Principle

Policy Statement

Information sharing shall be limited to the minimum amount of information reasonably necessary to accomplish the authorized purpose.

Objectives

Support:

- Privacy Protection
- Confidentiality
- Risk Reduction
- Regulatory Compliance

Requirements

- Recipients shall receive only information necessary to perform authorized activities.
- Excessive sharing is prohibited.

15.6 Internal Information Sharing

Policy Statement

Internal sharing shall be limited to authorized workforce members performing authorized activities.

Authorized Internal Recipients

Examples include where appropriate:

- Providers
- Care Teams
- Administrators
- Compliance Personnel
- Security Personnel
- Operations Personnel
- Executive Leadership

Controls

Examples include:

- RBAC
- Need-to-Know
- MFA
- Logging
- Monitoring

15.7 Covered Entity Information Sharing

Policy Statement

Information may be shared with Covered Entities to support authorized healthcare activities.

Examples

Covered Entities may include:

- Healthcare Providers
- Clinics
- Behavioral Health Organizations
- Wellness Organizations
- Hospitals
- Health Systems

Authorized Purposes

Examples include:

- Treatment
- Care Coordination
- Documentation
- Follow-Up Activities
- Healthcare Operations

Governance Requirements

Examples include:

- HIPAA Compliance
- Minimum Necessary

- Audit Logging
- Encryption

15.8 Provider and Care Team Sharing

Policy Statement

Information may be shared with authorized providers and care teams where necessary to support healthcare activities.

Examples

- Clinical Documentation
- Assessments
- Care Plans
- Treatment Plans
- Care Coordination Records
- Communications

Controls

Examples include:

- Access Controls
- Logging
- Monitoring
- Disclosure Controls

15.9 Business Associate Sharing

Policy Statement

Information may be shared with Business Associates where authorized and appropriate.

Requirements

Business Associates shall:

- Execute BAAs
- Protect PHI
- Protect ePHI
- Support Audits

- Report Incidents
- Support Retention Requirements

Governance Activities

Examples include:

- Due Diligence
- Risk Reviews
- Contract Reviews
- Monitoring

15.10 Vendor Information Sharing

Policy Statement

Information may be shared with vendors supporting authorized business activities.

Examples

- Cloud Providers
- Infrastructure Providers
- Security Providers
- Analytics Providers
- Communications Providers
- AI Providers

Vendor Requirements

Examples include:

- Privacy Controls
- Security Controls
- Access Controls
- Retention Controls
- Disposal Controls

Vendor Governance

Examples include:

- Due Diligence
- Risk Assessments
- Contract Reviews
- Monitoring

15.11 Subcontractor Sharing

Subcontractors receiving information shall be subject to:

- Privacy Requirements
- Security Requirements
- Contractual Requirements
- Monitoring Requirements
- Audit Requirements

Controls

Examples include:

- Access Restrictions
- Encryption
- Monitoring
- Logging

15.12 Cloud Service Provider Sharing

Policy Statement

Information may be processed within cloud environments supporting authorized services.

Requirements

Cloud providers shall support:

- Encryption
- Access Controls
- Logging
- Monitoring
- Backup Controls

- Disaster Recovery Controls

Governance Activities

Examples include:

- Security Reviews
- Privacy Reviews
- Risk Assessments
- Compliance Reviews

15.13 Managed Service Provider Sharing

MSPs may receive information necessary to support:

- Operations
- Infrastructure
- Monitoring
- Technical Support

Controls

Examples include:

- Least Privilege
- Monitoring
- Logging
- Access Reviews

15.14 Managed Security Service Provider Sharing

MSSPs may receive information necessary to support:

- Threat Detection
- Security Monitoring
- Incident Response
- Security Investigations

Examples

- Security Logs

- Authentication Logs
- Audit Logs
- Incident Records

Controls

Examples include:

- Monitoring
- Logging
- Access Controls
- Auditability

15.15 Customer-Directed Sharing

Policy Statement

Customers may authorize information sharing activities.

Examples

- API Integrations
- EHR Integrations
- Referrals
- Care Coordination
- Data Exports
- Third-Party Platforms

Governance Requirements

Examples include:

- Customer Authorization
- Documentation
- Logging
- Monitoring

15.16 API and Integration Sharing

Policy Statement

Information may be exchanged through approved APIs and integrations.

Examples

- EHR Systems
- Scheduling Systems
- Assessment Systems
- Analytics Systems
- Operational Systems

Controls

Examples include:

- Authentication
- Authorization
- Encryption
- Logging
- Monitoring

15.17 Artificial Intelligence Sharing

Policy Statement

Information shared with AI systems or AI vendors requires enhanced governance.

Governance Requirements

Examples include:

- Privacy Reviews
- Security Reviews
- AI Governance Reviews
- Risk Assessments
- Contract Reviews

Restrictions

Information shall not be shared with AI providers without appropriate governance approval.

15.18 Regulatory and Government Disclosures

Policy Statement

Cognera Health may disclose information where required or permitted by law.

Examples

- Regulatory Investigations
- Public Health Activities
- Healthcare Oversight Activities
- Government Requests
- Law Enforcement Requests
- Court Orders
- Subpoenas

Review Requirements

Disclosures shall be reviewed by where appropriate:

- **Legal Counsel**
- **Privacy Officer**
- **Compliance Officer**

15.19 Regulatory Authority Sharing

Information may be disclosed to where legally required:

- OCR
- HHS
- State Regulators
- Healthcare Regulators
- Privacy Regulators
- Government Agencies

Documentation

Regulatory disclosures shall be documented and retained.

15.20 Law Enforcement Disclosures

Policy Statement

Law enforcement disclosures shall be reviewed carefully and supported by appropriate authority.

Examples

- Warrants
- Court Orders
- Subpoenas
- Investigations

Controls

Examples include:

- Legal Review
- Documentation
- Logging
- Retention

15.21 Research and Analytics Disclosures

Policy Statement

Information may be used or disclosed for authorized research, analytics, product improvement, and quality improvement activities.

Governance Requirements

Examples include:

- De-Identification
- Anonymization
- Authorization
- Governance Review
- Privacy Review

Restrictions

Identifiable information shall not be disclosed without appropriate authority.

15.22 Cross-Border Transfers

Policy Statement

International transfers shall support applicable privacy and data protection requirements.

Safeguards

Examples include:

- Contractual Protections
- Security Controls
- Encryption
- Data Protection Reviews
- Risk Assessments

Related Policy

See: **Cross-Border Data Transfer Program**

15.23 Disclosure Accounting

Policy Statement

Disclosure records shall be maintained where required.

Examples

Records may include:

- Recipient
- Purpose
- Date
- Information Shared
- Legal Basis
- Authorization Basis

Retention

Disclosure records shall be retained according to approved retention schedules.

15.24 Sharing Risk Management

Risk Categories

Examples include:

- Unauthorized Disclosure
- Excessive Disclosure
- Vendor Risks
- AI Risks
- Regulatory Risks
- Cross-Border Risks

Risk Mitigation Activities

Examples include:

- Privacy Reviews
- Security Reviews
- Risk Assessments
- Audits
- Monitoring

15.25 Monitoring Program

Monitoring activities may include:

- Disclosure Monitoring
- Vendor Monitoring
- API Monitoring
- AI Sharing Monitoring
- Regulatory Disclosure Monitoring

Objectives

Identify:

- Unauthorized Sharing
- Excessive Sharing
- Control Failures

- Governance Gaps

15.26 Auditing Program

Audits may include:

- Privacy Audits
- Compliance Audits
- Vendor Audits
- AI Audits
- API Audits
- Disclosure Audits

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Control Effectiveness
- Risk Exposure

15.27 Information Sharing Metrics

Examples include:

- Disclosure Volume
- Vendor Sharing Reviews
- AI Sharing Reviews
- API Sharing Reviews
- Disclosure Findings
- Unauthorized Disclosure Events
- Regulatory Disclosure Activities

15.28 Prohibited Sharing Activities

Cognera Health prohibits:

- Unauthorized Sharing

- Excessive Sharing
- Unapproved Vendor Sharing
- Unapproved AI Sharing
- Sharing Without Appropriate Authority
- Sharing Without Required Authorization
- Sharing Contrary to Applicable Law

15.29 Roles and Responsibilities

Privacy Officer

Responsible for:

- Disclosure Governance
- Disclosure Reviews
- Privacy Escalations

Compliance Officer

Responsible for:

- Compliance Monitoring
- Regulatory Oversight

Legal Counsel

Responsible for:

- Legal Disclosures
- Regulatory Responses
- Court Orders
- Subpoenas

Steering Committee

Responsible for:

- Governance Oversight
- High-Risk Sharing Reviews

15.30 Continuous Improvement

Information sharing governance activities shall be reviewed periodically to improve:

- Privacy Protection
- Security Protection
- Regulatory Readiness
- Vendor Governance
- AI Governance
- Cross-Border Governance
- Accountability

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Major Technology Changes

The objective is to maintain a mature, auditable, transparent, accountable, privacy-conscious, and enterprise-grade Information Sharing Governance Program supporting all information exchange activities throughout the Cognera Health ecosystem.

16. HIPAA Privacy Practices, Protected Health Information Governance, Healthcare Information Protection, and HIPAA Compliance Program

16.1 Purpose

Purpose Statement

The purpose of this section is to establish the governance, privacy, security, compliance, accountability, oversight, monitoring, auditing, and operational requirements governing Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) processed by Cognera Health™.

As a healthcare technology organization supporting Covered Entities, healthcare providers, behavioral health organizations, wellness organizations, care teams, practitioners, and healthcare operations, Cognera Health recognizes that healthcare information requires enhanced protections due to its sensitive nature and the potential impact that misuse, unauthorized access, unauthorized disclosure, alteration, loss, or destruction may have on individuals and organizations.

This section establishes the HIPAA Privacy Governance Framework through which healthcare information is protected, managed, shared, retained, disclosed, audited, and governed.

16.2 Policy Statement

Cognera Health shall maintain administrative, technical, operational, organizational, contractual, and governance controls designed to support applicable obligations arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Breach Notification Rule
- HITECH Act
- Business Associate Obligations
- Customer Requirements
- Healthcare Privacy Requirements

PHI and ePHI shall be protected throughout their lifecycle.

All uses, disclosures, access, retention, sharing, transmission, storage, archival, deletion, destruction, and governance activities involving PHI and ePHI shall support applicable healthcare privacy requirements.

16.3 HIPAA Governance Objectives

The HIPAA Governance Program seeks to:

Protect PHI
Protect Protected Health Information from unauthorized access, disclosure, alteration, loss, misuse, or destruction.

Protect ePHI
Protect electronic Protected Health Information through administrative, technical, and operational safeguards.

Support Covered Entities
Support Covered Entities in meeting applicable healthcare obligations.

Support Individual Rights
Support privacy rights available under HIPAA.

Support Regulatory Compliance
Support compliance with applicable healthcare privacy requirements.

Reduce Risk
Reduce:

- Privacy Risk
- Security Risk
- Regulatory Risk
- Operational Risk
- Reputational Risk

Maintain Trust
Promote confidence among patients, providers, customers, and healthcare organizations.

16.4 Business Associate Governance

Policy Statement

Cognera Health generally operates as a Business Associate when processing PHI or ePHI on behalf of Covered Entities.

As a Business Associate, Cognera Health shall implement governance, privacy, security, monitoring, and compliance controls designed to support applicable Business Associate obligations.

Business Associate Responsibilities

Examples include:

- Protect PHI
- Protect ePHI

- Support Covered Entities
- Report Incidents
- Support Investigations
- Support Audits
- Support Regulatory Reviews
- Support Retention Requirements

Business Associate Agreements

Cognera Health shall maintain Business Associate Agreements where required.

BAAs may address:

- Permitted Uses
- Permitted Disclosures
- Security Obligations
- Incident Reporting
- Retention Requirements
- Disposal Requirements
- Audit Rights

16.5 Protected Health Information Governance

Definition

Protected Health Information (PHI) includes individually identifiable health information maintained or transmitted in any form.

Examples

- Clinical Documentation
- Treatment Plans
- Care Plans
- Assessments
- Behavioral Health Records
- Mental Health Records
- Substance Use Information
- Care Coordination Records
- Communications

- Wellness Information

Governance Requirements

PHI shall support:

- Enhanced Access Controls
- Encryption
- Monitoring
- Audit Logging
- Retention Controls
- Secure Disposal

16.6 Electronic Protected Health Information Governance

Definition

Electronic Protected Health Information (ePHI) includes PHI maintained, transmitted, processed, stored, archived, or accessed electronically.

Examples

- Databases
- Applications
- Backups
- Cloud Storage
- Analytics Platforms
- AI Systems
- Reporting Systems

Governance Requirements

ePHI shall support:

- Administrative Safeguards
- Technical Safeguards
- Operational Safeguards
- Security Monitoring
- Incident Response

16.7 Treatment Activities

Policy Statement

PHI may be used and disclosed to support treatment activities.

Examples

- Care Delivery
- Care Coordination
- Documentation
- Treatment Planning
- Follow-Up Activities
- Continuity of Care

HealScript™ Examples

- Clinical Documentation
- Assessments
- Treatment Plans
- Care Plans
- Referrals

HealConnect™ Examples

- Engagement Activities
- Assessments
- Communications
- Wellness Activities

Controls

Treatment-related uses shall support:

- Access Controls
- Minimum Necessary Requirements
- Audit Logging
- Monitoring

16.8 Payment Activities

Policy Statement

PHI may be used or disclosed to support authorized payment-related activities.

Examples

- Billing Activities
- Claims Activities
- Reimbursement Activities
- Eligibility Verification
- Financial Operations

Controls

Examples include:

- Minimum Necessary
- Access Controls
- Monitoring
- Audit Logging

16.9 Healthcare Operations Activities

Policy Statement

PHI may be used or disclosed to support authorized healthcare operations activities.

Examples

- Quality Improvement
- Outcome Measurement
- Compliance Activities
- Reporting
- Analytics
- Governance Reviews
- Workforce Management
- Operational Intelligence

Controls

Examples include:

- Access Controls
- Monitoring
- Audit Logging
- Governance Oversight

16.10 Minimum Necessary Standard

Policy Statement

Cognera Health shall support the HIPAA Minimum Necessary Standard.

Access, use, disclosure, sharing, transmission, and processing of PHI shall be limited to the minimum information reasonably necessary to accomplish the intended purpose.

Reference: 45 CFR §164.502(b)

Objectives

Support:

- Privacy Protection
- Confidentiality
- Risk Reduction
- Regulatory Compliance

Controls

Examples include:

- RBAC
- Need-to-Know
- Access Reviews
- Monitoring
- Logging

16.11 Uses and Disclosures Requiring Authorization

Policy Statement

Certain uses and disclosures of PHI require authorization.

Examples

- Marketing Activities
- Research Activities
- Certain AI Activities
- Certain Third-Party Disclosures
- Non-TPO Activities

Authorization Requirements
Authorizations should include:

- Description of Information
- Purpose
- Recipient
- Expiration
- Revocation Rights
- Signature or Equivalent Authorization

Governance Requirements

Examples include:

- Verification
- Documentation
- Retention
- Monitoring

16.12 Uses and Disclosures Not Requiring Authorization

Where permitted by law, certain uses and disclosures may occur without authorization.

Examples

- Treatment
- Payment

- Healthcare Operations
- Public Health Activities
- Health Oversight Activities
- Certain Law Enforcement Activities
- Regulatory Activities

Controls

Examples include:

- Minimum Necessary
- Documentation
- Monitoring
- Auditability

16.13 Accounting of Disclosures

Policy Statement

Cognera Health shall support accounting of disclosures requirements where applicable.

Disclosure Records

Examples include:

- Recipient
- Purpose
- Date
- Information Shared
- Legal Basis
- Authorization Basis

Retention

Disclosure records shall be retained according to approved retention schedules.

16.14 Confidential Communications

Policy Statement

Individuals may request confidential communications where applicable.

Examples

- Alternative Contact Methods
- Alternative Addresses
- Restricted Communications

Governance Requirements
Requests shall be reviewed and documented.

16.15 Restrictions Requests

Policy Statement

Individuals may request restrictions on certain uses or disclosures where applicable.

Examples

- Disclosure Restrictions
- Sharing Restrictions
- Communication Restrictions

Review Requirements

Requests shall be evaluated according to:

- Legal Requirements
- Customer Requirements
- Operational Requirements

16.16 Individual Access Rights

Policy Statement

Individuals may request access to information where legally permitted.

Examples

- Clinical Records
- Assessments
- Communications
- Wellness Information

- Behavioral Health Information

Verification Requirements

Examples include:

- Identity Verification
- Authorization Validation
- Representative Validation

Documentation
Requests shall be documented and retained.

16.17 Amendment Rights

Policy Statement

Individuals may request correction or amendment of information where applicable.

Examples

- Incorrect Information
- Incomplete Information
- Outdated Information

Governance Requirements

Requests shall be:

- Reviewed
- Validated
- Documented
- Resolved

16.18 Complaint Rights

Policy Statement

Individuals may submit privacy complaints.

Examples

- Privacy Concerns
- Disclosure Concerns
- Access Concerns
- Rights Concerns
- Security Concerns

Governance Requirements

Complaints shall be:

- Logged
- Investigated
- Evaluated
- Resolved

16.19 Workforce HIPAA Responsibilities

All workforce members shall:

- Protect PHI
- Protect ePHI
- Follow Policies
- Complete Training
- Report Incidents
- Support Investigations
- Support Audits
- Support Compliance Activities

Training Requirements

Examples include:

- HIPAA Privacy Training
- HIPAA Security Training
- Incident Reporting Training
- Privacy Awareness Training

16.20 Security Requirements Supporting HIPAA

Examples include:

- Encryption
- MFA
- RBAC
- Logging
- Monitoring
- Vulnerability Management
- Incident Response
- Backup Management
- Disaster Recovery

16.21 HIPAA Risk Management Program

Policy Statement

Healthcare-related risks shall be evaluated periodically.

Risk Categories

Examples include:

- Unauthorized Access
- Unauthorized Disclosure
- Improper Sharing
- Vendor Risks
- AI Risks
- Retention Risks
- Security Risks

Risk Mitigation Activities

Examples include:

- Risk Assessments
- Privacy Reviews
- Security Reviews
- Vendor Reviews

- Corrective Actions

16.22 Monitoring Program

Monitoring activities may include:

- Access Monitoring
- Disclosure Monitoring
- Security Monitoring
- Vendor Monitoring
- AI Monitoring
- Rights Monitoring

Objectives

Identify:

- Unauthorized Access
- Unauthorized Disclosure
- Noncompliance
- Governance Gaps

16.23 Auditing Program

Audits may include:

- HIPAA Audits
- Privacy Audits
- Security Audits
- Vendor Audits
- AI Governance Audits
- Disclosure Audits

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness

- Control Effectiveness
- Risk Exposure

16.24 HIPAA Metrics

Examples include:

- HIPAA Incidents
- Disclosure Reviews
- Access Review Completion
- Rights Request Volume
- Audit Findings
- Vendor Findings
- AI Governance Findings

16.25 Roles and Responsibilities

Privacy Officer

Responsible for:

- HIPAA Governance
- Privacy Reviews
- Incident Reviews

Compliance Officer

Responsible for:

- Compliance Monitoring
- Audit Coordination

Legal Counsel

Responsible for:

- Legal Interpretation
- Regulatory Responses

Steering Committee

Responsible for:

- Governance Oversight
- Risk Oversight

16.26 Continuous Improvement

The HIPAA Governance Program shall be periodically reviewed to improve:

- Privacy Protection
- Security Protection
- Compliance Readiness
- Governance Maturity
- Workforce Awareness
- Vendor Governance
- AI Governance

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Significant Business Changes

The objective is to maintain a mature, auditable, scalable, healthcare-focused, and enterprise-grade HIPAA Privacy Governance Program supporting the protection of healthcare information throughout the Cognera Health ecosystem.

17. Privacy Rights Management Program, Individual Rights Governance, Rights Request Administration, and Consumer Privacy Rights Framework

17.1 Purpose

Purpose Statement

The purpose of this section is to establish a comprehensive Privacy Rights Management Program governing the receipt, verification, review, processing, fulfillment, denial, escalation, documentation, auditing, and reporting of privacy rights requests.

Cognera Health™ recognizes that privacy rights are a fundamental component of privacy governance, transparency, accountability, trust, and regulatory compliance.

This program is intended to provide individuals with appropriate mechanisms to exercise applicable rights regarding information collected, processed, stored, shared, retained, disclosed, transferred, and otherwise managed by Cognera Health.

The Privacy Rights Program supports applicable rights arising from:

- HIPAA
- HITECH
- GDPR
- UK GDPR
- CCPA
- CPRA
- Consumer Health Data Laws
- State Privacy Laws
- Contractual Requirements
- Customer Requirements

17.2 Policy Statement

Cognera Health shall maintain formal processes supporting applicable privacy rights requests.

Privacy rights activities shall be:

- Transparent
- Accessible
- Consistent
- Auditable
- Verifiable
- Documented
- Governed
- Monitored

Privacy rights requests shall be reviewed in a timely, fair, objective, and consistent manner.

The organization shall maintain governance controls supporting the identification, validation, fulfillment, denial, escalation, reporting, and monitoring of rights requests.

17.3 Privacy Rights Governance Objectives

The Privacy Rights Program seeks to:

Support Individual Rights
Enable individuals to exercise applicable privacy rights.

Promote Transparency
Provide visibility into information processing activities.

Support Accountability
Ensure requests are documented and auditable.

Support Regulatory Compliance
Support applicable privacy requirements.

Reduce Privacy Risk
Reduce risks associated with improper rights handling.

Maintain Trust
Promote confidence in privacy governance activities.

17.4 Privacy Rights Governance Principles

All rights activities shall support:

- Transparency
- Accessibility
- Fairness
- Accountability
- Verification
- Documentation
- Auditability
- Timeliness

- Security

17.5 Privacy Rights Governance Framework

The Privacy Rights Program consists of:

- Access Rights Governance
- Correction Rights Governance
- Deletion Rights Governance
- Restriction Rights Governance
- Portability Rights Governance
- Objection Rights Governance
- Consent Withdrawal Governance
- HIPAA Rights Governance
- Consumer Health Data Rights Governance
- Appeals Governance
- Complaint Governance
- Rights Monitoring and Reporting

17.6 Rights Request Intake Program

Policy Statement

Cognera Health shall maintain mechanisms allowing authorized individuals to submit privacy rights requests.

Request Channels

Examples include:

- Privacy Office
  - privacy@cogneraheath.ai
- Customer Administrator
- Authorized Representative
- Privacy Portal
- Written Requests
- Customer Support Channels

Supported Request Types

Examples include:

- Access Requests
- Correction Requests
- Deletion Requests
- Restriction Requests
- Portability Requests
- Objection Requests
- Consent Withdrawal Requests
- Complaint Requests
- Appeal Requests

17.7 Identity Verification Program

Policy Statement

Identity verification is required before fulfilling rights requests.

Objectives

Protect against:

- Unauthorized Disclosure
- Fraud
- Impersonation
- Unauthorized Access

Verification Activities

Examples include:

- Identity Verification
- Account Verification
- Authorization Validation
- Representative Validation

Additional Verification

Additional verification may be required where:

- Sensitive Information Is Involved
- High-Risk Requests Are Involved
- Regulatory Requirements Apply

17.8 Right of Access

Policy Statement

Individuals may request access to information concerning them where legally permitted.

Objectives

Support:

- Transparency
- Accountability
- Individual Rights

Examples

Information may include where legally permissible:

- Personal Information
- Consumer Health Data
- Assessment Information
- Communications
- Wellness Information
- Behavioral Health Information

Access Controls

Examples include:

- Identity Verification
- Authorization Validation
- Secure Delivery
- Audit Logging

Exceptions

Access may be restricted where:

- Legal Restrictions Apply
- Security Risks Exist
- Regulatory Exceptions Apply
- Investigations Are Active

17.9 Right to Rectification (Correction)

Policy Statement

Individuals may request correction of inaccurate information where applicable.

Examples

- Incorrect Personal Information
- Incorrect Contact Information
- Administrative Errors
- Incomplete Information

Governance Requirements

Correction requests shall be:

- Reviewed
- Validated
- Documented
- Audited

Restrictions
Certain records may not be modified where prohibited by law or regulation.

17.10 Right to Erasure (Deletion)

Policy Statement

Individuals may request deletion of information where legally permissible.

Objectives

Support:

- Privacy Protection

- Data Minimization
- Storage Limitation

Review Requirements

Requests shall be evaluated against:

- Retention Requirements
- Legal Obligations
- Regulatory Requirements
- Security Obligations
- Continuity of Care Requirements
- Investigations
- Legal Holds

Exceptions

Deletion may be denied where:

- HIPAA Requirements Apply
- Legal Holds Exist
- Litigation Exists
- Regulatory Investigations Exist
- Security Obligations Exist

17.11 Right to Restrict Processing

Policy Statement

Individuals may request restrictions regarding certain processing activities where applicable.

Examples

- Certain Disclosures
- Certain Sharing Activities
- Certain Analytics Activities
- Certain AI Activities

Review Activities

Requests shall be reviewed according to:

- Legal Requirements
- Customer Requirements
- Operational Requirements

17.12 Right to Data Portability

Policy Statement

Individuals may request portable copies of information where applicable.

Examples

- Personal Information
- Consumer Health Data
- Assessment Information
- Wellness Information
- Communications

Governance Requirements

Examples include:

- Verification
- Secure Export
- Encryption
- Audit Logging

17.13 Right to Object

Policy Statement

Individuals may object to certain processing activities where applicable.

Examples

- Analytics Activities
- Certain Sharing Activities
- Certain Processing Activities

- Certain Marketing Activities

Governance Requirements
Requests shall be evaluated according to applicable requirements.

17.14 Consent Withdrawal Governance

Policy Statement

Individuals may withdraw consent where legally permissible.

Examples

- AI Consent
- Voice Consent
- Marketing Consent
- Recording Consent
- Consumer Health Data Consent

Effects of Withdrawal

Withdrawal may:

- Limit Features
- Restrict Functionality
- Restrict Participation
- Restrict Processing

Activities Not Affected

Withdrawal generally does not affect:

- Prior Lawful Processing
- Legal Obligations
- Security Obligations
- Retention Obligations

17.15 HIPAA Privacy Rights Governance

Where applicable, individuals may exercise rights including:

- Access

- Amendment
- Restrictions
- Accounting of Disclosures
- Confidential Communications

Governance Requirements

Requests shall support:

- Verification
- Documentation
- Auditability
- Timely Response

17.16 GDPR Rights Governance

Where applicable:

- Article 15 – Access
- Article 16 – Rectification
- Article 17 – Erasure
- Article 18 – Restriction
- Article 20 – Portability
- Article 21 – Objection

Governance Requirements

Examples include:

- Documentation
- Verification
- Audit Logging
- Regulatory Compliance

17.17 UK GDPR Rights Governance

Where applicable, substantially similar rights shall be supported.

Examples include:

- Access
- Rectification
- Erasure
- Restriction
- Portability
- Objection

17.18 Consumer Health Data Rights Governance

Policy Statement

Consumer health data rights shall be supported where applicable.

Examples

- Access
- Deletion
- Restriction
- Consent Withdrawal
- Sharing Restrictions

Governance Requirements

Examples include:

- Verification
- Documentation
- Monitoring
- Auditing

17.19 Authorized Representative Requests

Policy Statement

Authorized representatives may submit requests where legally authorized.

Examples

- Parents
- Legal Guardians

- Attorneys
- Authorized Representatives

Verification Requirements
Representatives shall provide evidence of authority where required.

17.20 Appeals Program

Policy Statement

Where applicable, individuals may appeal privacy-related decisions.

Examples

- Access Denials
- Deletion Denials
- Restriction Denials
- Correction Denials

Review Authorities

Appeals may be reviewed by:

- Privacy Officer
- Compliance Officer
- Legal Counsel

17.21 Complaint Governance

Individuals may submit complaints regarding:

- Privacy Practices
- Rights Requests
- Disclosure Activities
- Consent Activities
- Security Concerns

Complaint Activities

Complaints shall be:

- Logged
- Investigated

- Evaluated
- Resolved

17.22 Rights Request Service Levels

Objectives

Rights requests should be processed within applicable regulatory timelines.

Monitoring Areas

Examples include:

- Response Time
- Resolution Time
- Escalation Time
- Closure Time

Governance Requirement
Applicable legal and regulatory timelines shall govern response obligations.

17.23 Rights Documentation Requirements

Request records may include:

- Request Type
- Request Date
- Verification Activities
- Resolution Activities
- Communications
- Escalations
- Appeals
- Closure Information

Retention
Rights records shall be retained according to approved retention schedules.

17.24 Monitoring Program

Monitoring activities may include:

- Access Requests
- Deletion Requests
- Appeals
- Complaints
- Verification Activities
- SLA Compliance

Objectives

Identify:

- Delays
- Noncompliance
- Control Gaps
- Process Inefficiencies

17.25 Auditing Program

Audits may include:

- Rights Audits
- HIPAA Rights Audits
- Consumer Health Data Rights Audits
- Complaint Audits
- Appeal Audits

Audit Objectives

Evaluate:

- Compliance
- Timeliness
- Documentation Quality
- Governance Effectiveness

17.26 Privacy Rights Metrics

Examples include:

- Request Volume
- Access Requests
- Deletion Requests
- Correction Requests
- Appeal Volume
- Complaint Volume
- SLA Compliance
- Audit Findings

17.27 Roles and Responsibilities

Privacy Officer

Responsible for:

- Rights Governance
- Appeals
- Escalations
- Reporting

Compliance Officer

Responsible for:

- Compliance Monitoring
- Auditing
- Regulatory Readiness

Legal Counsel

Responsible for:

- Legal Interpretation
- Escalation Support

Steering Committee

Responsible for:

- Governance Oversight
- High-Risk Reviews

17.28 Continuous Improvement

The Privacy Rights Program shall be periodically reviewed to improve:

- Transparency
- Accessibility
- Timeliness
- Compliance
- Governance Maturity
- Customer Trust

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Major Operational Changes

The objective is to maintain a mature, transparent, auditable, compliant, and enterprise-grade Privacy Rights Management Program supporting all applicable individual privacy rights throughout the Cognera Health ecosystem.

18. California Privacy Rights, Consumer Health Data Rights, State Privacy Rights, Sensitive Personal Information Governance, and Consumer Data Protection Program

18.1 Purpose

Purpose Statement

The purpose of this section is to establish a comprehensive governance framework supporting privacy rights, consumer health data protections, sensitive personal

information protections, transparency obligations, consent requirements, disclosure controls, and consumer protections arising from California privacy laws, consumer health data laws, and other applicable U.S. state privacy regulations.

Cognera Health™ recognizes that privacy regulation within the United States continues to evolve rapidly and that organizations processing personal information, consumer health data, wellness information, behavioral health information, and related sensitive information must implement governance controls supporting enhanced transparency, accountability, and individual rights.

This section establishes governance requirements supporting:

- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Consumer Health Data Laws
- Washington My Health My Data Act
- Texas Data Privacy and Security Act
- Emerging State Privacy Laws
- Consumer Protection Requirements

18.2 Policy Statement

Cognera Health shall maintain policies, procedures, controls, monitoring activities, auditing activities, and governance mechanisms supporting applicable state privacy rights and consumer protections.

The organization shall provide individuals with reasonable mechanisms to:

- Understand information processing activities.
- Exercise applicable privacy rights.
- Request information.
- Request corrections.
- Request deletion.
- Request restrictions.
- Submit complaints.
- Appeal decisions.

All consumer privacy activities shall support:

- Transparency

- Accountability
- Privacy Protection
- Consumer Trust
- Regulatory Compliance

18.3 Consumer Privacy Governance Objectives

The Consumer Privacy Program seeks to:

Promote Transparency
Provide visibility into information collection and processing practices.

Support Individual Control
Enable individuals to exercise applicable privacy rights.

Protect Consumer Health Data
Provide enhanced protections for health-related information.

Protect Sensitive Personal Information
Apply heightened protections to sensitive information.

Reduce Risk
Reduce:

- Privacy Risk
- Regulatory Risk
- Consumer Harm
- Reputational Risk

Support Compliance
Support applicable state privacy obligations.

18.4 California Privacy Governance

California Consumer Privacy Act (CCPA)

Purpose

The CCPA establishes privacy rights for California residents concerning personal information.

Governance Objectives

Support:

- Right to Know
- Right to Access
- Right to Delete
- Right to Information
- Non-Discrimination
- Transparency

Organizational Commitments

Cognera Health shall maintain processes supporting applicable California privacy rights.

18.5 California Privacy Rights Act (CPRA)

Purpose

The CPRA expands California privacy protections and introduces additional consumer rights.

Additional Rights

Examples include:

- Right to Correct
- Right to Limit Sensitive Personal Information
- Expanded Transparency
- Enhanced Consumer Protections

Governance Requirements

CPRA-related activities shall support:

- Documentation
- Monitoring
- Auditing
- Rights Management
- Governance Oversight

18.6 Right to Know Governance

Policy Statement

Where applicable, individuals may request information regarding personal information collected, processed, disclosed, retained, or shared.

Examples

Information may include:

- Categories Collected
- Sources
- Purposes
- Sharing Activities
- Retention Practices
- Third-Party Recipients

Governance Requirements

Examples include:

- Identity Verification
- Documentation
- Audit Logging
- Secure Delivery

18.7 Right to Access Governance

Policy Statement

Individuals may request access to applicable personal information.

Objectives

Support:

- Transparency
- Accountability
- Individual Rights

Examples

- Personal Information
- Consumer Health Data
- Wellness Information
- Communications
- Assessment Information

Controls

Examples include:

- Verification
- Authorization Validation
- Secure Transmission
- Documentation

18.8 Right to Delete Governance

Policy Statement

Individuals may request deletion of personal information where legally permissible.

Review Requirements

Requests shall be evaluated against:

- Retention Requirements
- Legal Obligations
- Regulatory Requirements
- Security Obligations
- Investigations
- Legal Holds
- Continuity-of-Care Requirements

Exceptions
Deletion may be denied where retention remains required.

Documentation
Deletion requests shall be documented and retained.

18.9 Right to Correct Governance

Policy Statement

Individuals may request correction of inaccurate personal information.

Examples

- Incorrect Contact Information
- Administrative Errors
- Incomplete Information
- Outdated Information

Governance Requirements

Correction requests shall be:

- Reviewed
- Validated
- Documented
- Audited

18.10 Right to Limit Sensitive Personal Information

Policy Statement

Where applicable, individuals may request limitations regarding the use of Sensitive Personal Information.

Examples

Sensitive information may include:

- Consumer Health Data
- Behavioral Health Information
- Wellness Information
- Government Identifiers
- Geolocation Information
- Authentication Information

Governance Requirements

Requests shall be evaluated according to applicable legal requirements.

18.11 Non-Discrimination Governance

Policy Statement

Cognera Health shall not unlawfully discriminate against individuals for exercising privacy rights.

Examples

Individuals shall not be denied lawful privacy rights due to:

- Access Requests
- Deletion Requests
- Correction Requests
- Complaints
- Appeals

Governance Requirements
Non-discrimination requirements shall be monitored periodically.

18.12 Sensitive Personal Information Governance

Policy Statement

Sensitive Personal Information (SPI) shall receive enhanced protections.

Examples

- Health Information
- Behavioral Health Information
- Consumer Health Data
- Government Identifiers
- Authentication Credentials
- Financial Information
- Biometric Information

Enhanced Controls

Examples include:

- Encryption
- Access Controls
- Monitoring
- Audit Logging
- Retention Controls
- Disposal Controls

18.13 Consumer Health Data Governance

Policy Statement

Consumer health data requires enhanced governance due to its sensitivity.

Examples

Consumer health data may include:

- Mood Information
- Wellness Information
- Recovery Activities
- Symptom Information
- Behavioral Health Information
- Journaling Information
- Assessment Information

Governance Requirements

Examples include:

- Transparency
- Consent
- Access Controls
- Monitoring
- Auditing
- Rights Support

18.14 Washington My Health My Data Act Governance

Purpose

Support governance obligations arising from Washington consumer health data requirements.

Governance Areas

Examples include:

- Collection
- Processing
- Sharing
- Consent
- Retention
- Deletion
- Consumer Rights

Monitoring
Privacy leadership shall monitor regulatory developments and adjust controls where necessary.

18.15 State Privacy Law Governance

Policy Statement

Cognera Health recognizes that privacy obligations may arise from multiple state privacy laws.

Examples

- California
- Texas
- Colorado
- Connecticut
- Virginia
- Utah
- Washington
- Emerging State Privacy Laws

Governance Objectives

Support:

- Transparency
- Accountability
- Consumer Rights
- Consumer Protection
- Regulatory Compliance

18.16 Authorized Agent Governance

Policy Statement

Authorized agents may submit privacy requests on behalf of individuals where legally authorized.

Examples

- Attorneys
- Legal Guardians
- Parents
- Authorized Representatives

Verification Requirements
Authorized agents shall provide evidence of authority where required.

18.17 Consumer Complaints Program

Individuals may submit complaints regarding:

- Privacy Practices
- Consumer Health Data Activities
- Rights Requests
- Sharing Activities
- Consent Activities

Complaint Activities

Complaints shall be:

- Logged
- Investigated
- Evaluated
- Resolved

18.18 Appeals Governance

Policy Statement

Where applicable, individuals may appeal privacy-related decisions.

Examples

- Access Denials
- Deletion Denials
- Correction Denials
- Restriction Denials

Review Authorities

Appeals may be reviewed by:

- Privacy Officer
- Compliance Officer
- Legal Counsel

18.19 Consumer Data Risk Management

Risk Categories

Examples include:

- Unauthorized Disclosure
- Excessive Collection
- Improper Sharing
- Consent Failures
- Rights Failures
- Vendor Risks
- AI Risks

Mitigation Activities

Examples include:

- Monitoring
- Auditing
- Reviews
- Corrective Actions
- Governance Oversight

18.20 Monitoring Program

Monitoring activities may include:

- Rights Requests
- Consumer Complaints
- Consumer Health Data Activities
- Sensitive Information Activities
- Consent Activities
- Vendor Activities

Objectives

Identify:

- Noncompliance
- Delays
- Rights Failures
- Governance Gaps

18.21 Auditing Program

Audits may include:

- Consumer Rights Audits
- Consumer Health Data Audits
- Privacy Audits
- Consent Audits

- Vendor Audits

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Rights Management
- Risk Exposure

18.22 Consumer Privacy Metrics

Examples include:

- Rights Request Volume
- Deletion Requests
- Correction Requests
- Consumer Complaints
- Appeals
- Consent Compliance
- Consumer Health Data Findings
- Audit Findings

18.23 Roles and Responsibilities

Privacy Officer

Responsible for:

- Consumer Privacy Governance
- Rights Oversight
- Complaint Management

Compliance Officer

Responsible for:

- Compliance Monitoring
- Regulatory Readiness

Legal Counsel

Responsible for:

- Legal Interpretation
- Escalation Support

Data Governance Steering Committee

Responsible for:

- Governance Oversight
- High-Risk Reviews

18.24 Continuous Improvement

The Consumer Privacy Governance Program shall be periodically reviewed to improve:

- Transparency
- Consumer Protection
- Privacy Rights Management
- Consumer Health Data Protection
- Compliance Readiness
- Governance Maturity

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Significant Business Changes

The objective is to maintain a mature, transparent, auditable, consumer-focused, privacy-conscious, and enterprise-grade Consumer Privacy Governance Program supporting evolving state privacy requirements throughout the Cognera Health ecosystem.

19. Artificial Intelligence Governance, Responsible AI Program, AI Risk Management, Model Governance, and Intelligent Systems Oversight Framework

19.1 Purpose

Purpose Statement

The purpose of this section is to establish the enterprise governance framework governing the design, acquisition, development, implementation, validation, deployment, operation, monitoring, maintenance, retirement, oversight, auditing, and continuous improvement of Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP), Natural Language Understanding (NLU), Predictive Analytics, Generative AI, Large Language Models (LLMs), Intelligent Automation, and AI-enabled technologies utilized throughout the Cognera Health™ ecosystem.

Artificial Intelligence technologies have the potential to significantly improve healthcare operations, behavioral health workflows, wellness engagement, documentation quality, operational efficiency, care coordination, reporting, analytics, and decision support capabilities.

At the same time, AI introduces unique privacy, security, ethical, clinical, legal, operational, and regulatory risks that require specialized governance beyond traditional information technology governance.

This section establishes a comprehensive Responsible AI Program designed to ensure that AI systems are:

- Safe
- Responsible
- Transparent
- Explainable
- Auditable
- Accountable
- Ethical
- Privacy-Conscious
- Secure
- Human-Governed

19.2 Policy Statement

Cognera Health shall maintain a formal Artificial Intelligence Governance Program governing all AI-enabled technologies utilized by the organization.

AI systems shall operate within established governance, privacy, security, compliance, risk management, monitoring, validation, auditing, and oversight frameworks.

Artificial Intelligence technologies shall support and augment human decision-making.

AI technologies shall not replace:

- Clinical Judgment
- Professional Judgment
- Human Accountability
- Organizational Accountability
- Regulatory Responsibilities
- Governance Responsibilities

Final responsibility for decisions remains with authorized individuals and organizations.

19.3 Responsible AI Mission

The mission of the Responsible AI Program is to ensure that AI technologies are deployed in a manner that:

- Benefits individuals.
- Benefits providers.
- Benefits organizations.
- Supports healthcare delivery.
- Supports wellness activities.
- Supports responsible innovation.
- Protects privacy.
- Protects security.
- Preserves trust.

The organization recognizes that responsible AI governance is an ongoing commitment rather than a one-time activity.

19.4 Responsible AI Principles

Human-Centered AI

- AI technologies shall be designed and deployed to support human decision-making.
- Humans remain responsible for decisions.

Human-in-the-Loop

- Appropriate human oversight shall be maintained throughout AI-enabled workflows.
- Humans shall have the ability to:
    - Review Outputs
    - Validate Outputs
    - Modify Outputs
    - Reject Outputs
    - Override Outputs

Transparency

Users should understand:

- When AI is used.
- Why AI is used.
- What AI is doing.
- What limitations exist.

Explainability

AI-generated outputs should be understandable to the extent reasonably feasible.

Fairness

AI systems shall be monitored for:

- Bias
- Discrimination
- Disparate Impact
- Unintended Outcomes

Accountability

- Responsibility remains with humans and organizations.
- AI systems do not assume accountability.

Privacy Protection

AI systems shall support:

- Data Minimization
- Privacy by Design
- Purpose Limitation
- Consent Requirements

Security Protection

AI systems shall support:

- Secure Processing
- Access Controls
- Monitoring
- Logging
- Risk Management

19.5 AI Governance Framework

The AI Governance Program consists of:

- AI Inventory Management
- AI Risk Management
- AI Validation
- AI Monitoring
- AI Auditing
- AI Incident Management
- AI Security
- AI Vendor Governance
- AI Lifecycle Management
- AI Change Management
- AI Ethics Oversight
- AI Regulatory Readiness

19.6 AI Governance Structure

Executive Leadership

Responsible for:

- Strategic Oversight
- Enterprise AI Risk Oversight
- AI Investment Decisions

Privacy Officer

Responsible for:

- AI Privacy Oversight
- AI Risk Reviews
- AI Privacy Controls

Compliance Officer

Responsible for:

- Regulatory Monitoring
- AI Compliance Oversight

CISO

Responsible for:

- AI Security Oversight
- AI Security Controls

Legal Counsel

Responsible for:

- AI Legal Review
- Regulatory Interpretation

Data Governance Steering Committee

Responsible for:

- AI Governance Oversight
- AI Risk Oversight
- AI Policy Approval

AI Governance Owner

Responsible for:

- Day-to-Day Program Management
- AI Inventory Management
- Validation Coordination

19.7 AI Inventory Program

Policy Statement

Cognera Health shall maintain a comprehensive inventory of AI systems.

Inventory Requirements

Each AI system should have documented:

- System Name
- Description
- Business Purpose
- Owner
- Vendor
- Inputs
- Outputs
- Risk Classification
- Validation Status
- Deployment Status
- Retirement Status

Inventory Reviews

Inventories shall be reviewed:

- Quarterly
- Following AI Deployments
- Following AI Retirements

19.8 AI Risk Classification Framework

Purpose

All AI systems shall be classified according to risk.

Low Risk AI

Examples:

- Administrative Automation
- Internal Productivity Tools
- Non-Sensitive Reporting

Moderate Risk AI

Examples:

- Operational Analytics
- Reporting Assistance
- Workflow Assistance

High Risk AI

Examples:

- Clinical Documentation Assistance
- Behavioral Health Intelligence
- Engagement Intelligence
- Care Coordination Intelligence

Critical Risk AI

Examples:

- High-Impact Predictive Systems
- Population-Level Clinical Intelligence
- Regulatory-Sensitive AI Systems

Governance Requirements
Higher risk classifications require:

- Additional Validation
- Additional Monitoring
- Additional Review
- Additional Approval

19.9 AI Approval Governance

Policy Statement

AI systems shall not be deployed without appropriate review and approval.

Review Activities

Examples include:

- Privacy Review
- Security Review
- Compliance Review
- Risk Review
- Legal Review
- Governance Review

Approval Authorities

May include depending upon risk level:

- **Privacy Officer**
- **Compliance Officer**
- **CISO**
- **Steering Committee**
- **Executive Leadership**

19.10 AI Model Governance

Policy Statement

All AI models shall be governed throughout their lifecycle.

Model Governance Areas

Examples include:

- Model Design
- Model Development
- Model Testing
- Model Validation
- Model Deployment

- Model Monitoring
- Model Retirement

Governance Objectives

Ensure:

- Reliability
- Accuracy
- Consistency
- Accountability
- Traceability

19.11 AI Training Data Governance

Policy Statement

Training datasets require enhanced governance.

Objectives

Ensure:

- Data Quality
- Data Integrity
- Privacy Protection
- Security Protection
- Bias Mitigation

Requirements

Training datasets shall be reviewed for:

- Appropriateness
- Accuracy
- Relevance
- Legal Use
- Privacy Compliance

Restrictions

PHI shall not be used for AI model training unless specifically authorized and approved.

19.12 AI Validation Program

Policy Statement

AI systems shall undergo formal validation.

Validation Objectives

Evaluate:

- Accuracy
- Reliability
- Consistency
- Fairness
- Safety
- Explainability
- Performance

Validation Activities

Examples include:

- Functional Testing
- Clinical Review
- Security Review
- Privacy Review
- Output Review
- Bias Review

Validation Documentation

Examples include:

- Validation Reports
- Test Results
- Approval Records
- Monitoring Plans

19.13 Human-in-the-Loop Governance

Policy Statement

Human oversight is required for AI-enabled activities involving healthcare, behavioral health, consumer health, documentation, recommendations, and decision support.

Human Responsibilities

Examples include:

- Review Outputs
- Validate Outputs
- Approve Outputs
- Reject Outputs
- Override Outputs
- Escalate Concerns

Clinical Restrictions
AI-generated outputs shall not be relied upon without appropriate review.

19.14 AI Monitoring Program

Policy Statement

AI systems shall undergo ongoing monitoring.

Monitoring Objectives

Monitor:

- Accuracy
- Reliability
- Performance
- Drift
- Bias
- Security
- Privacy

Monitoring Activities

Examples include:

- Output Reviews
- Trend Analysis
- Error Analysis
- User Feedback
- Incident Monitoring

19.15 AI Bias Management Program

Policy Statement

AI systems shall be monitored for potential bias.

Sources of Bias

Examples include:

- Training Data Bias
- Sampling Bias
- Labeling Bias
- Representation Bias
- Algorithmic Bias

Mitigation Activities

Examples include:

- Validation
- Monitoring
- Human Review
- Governance Reviews
- Corrective Actions

19.16 AI Security Program

Threat Categories

Examples include:

- Prompt Injection
- Data Leakage

- Model Manipulation
- Unauthorized Access
- Adversarial Inputs
- Training Data Exposure

Security Controls

Examples include:

- Encryption
- MFA
- RBAC
- Logging
- Monitoring
- Vulnerability Management

19.17 AI Incident Management

AI Incidents

Examples include:

- Hallucinations
- Inaccurate Outputs
- Privacy Violations
- Bias Findings
- Security Events
- Unauthorized Processing

Response Activities

Examples include:

- Investigation
- Containment
- Remediation
- Monitoring
- Governance Review

19.18 AI Change Management

Policy Statement

Material AI changes shall undergo governance review.

Examples

- Model Updates
- Prompt Changes
- Vendor Changes
- Training Data Changes
- Infrastructure Changes

Review Requirements

Examples include:

- Privacy Review
- Security Review
- Risk Review
- Validation Review

19.19 AI Vendor Governance

Policy Statement

Third-party AI providers require enhanced governance.

Review Activities

Examples include:

- Privacy Assessments
- Security Assessments
- Risk Assessments
- Contract Reviews
- AI Governance Reviews

Vendor Requirements

Examples include:

- Privacy Controls
- Security Controls
- Audit Support
- Transparency
- Monitoring

19.20 AI Auditing Program

Policy Statement

AI systems shall be auditable.

Audit Areas

Examples include:

- Inputs
- Outputs
- Validation
- Monitoring
- Human Review
- Overrides
- Incidents

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Control Effectiveness
- Risk Exposure

19.21 AI Metrics and Reporting

Examples include:

- Validation Completion Rates
- Human Review Rates

- Override Rates
- Drift Findings
- Bias Findings
- AI Incidents
- AI Audit Findings
- AI Adoption Metrics

Reporting Recipients

Examples include:

- Privacy Officer
- Compliance Officer
- CISO
- Steering Committee
- Executive Leadership

19.22 AI Regulatory Readiness

Cognera Health shall monitor:

- AI Regulations
- Healthcare AI Guidance
- State AI Laws
- International AI Requirements
- Industry Best Practices

Objectives

Maintain:

- Compliance Readiness
- Governance Maturity
- Responsible Innovation

19.23 AI Lifecycle Management

AI systems shall be governed throughout:

- Design
- Development
- Testing
- Validation
- Deployment
- Monitoring
- Retirement

Governance Reviews

Each stage may require:

- Privacy Review
- Security Review
- Compliance Review
- Legal Review
- Risk Review

19.24 AI Retirement Program

Policy Statement

Retired AI systems shall undergo controlled decommissioning.

Activities

Examples include:

- Access Removal
- Inventory Updates
- Monitoring Termination
- Documentation Preservation
- Secure Disposal

19.25 Continuous Improvement

The Responsible AI Program shall be periodically reviewed to improve:

- Transparency

- Explainability
- Accountability
- Fairness
- Privacy Protection
- Security Protection
- Governance Maturity
- Regulatory Readiness

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Significant AI Changes

The objective is to maintain a mature, transparent, explainable, secure, privacy-conscious, ethically governed, and enterprise-grade Responsible AI Program supporting all AI-enabled activities throughout the Cognera Health ecosystem.

20. Cross-Border Data Transfers, International Processing, Data Residency, Global Privacy Governance, and International Data Protection Program

20.1 Purpose

Purpose Statement

The purpose of this section is to establish the governance framework governing international processing, cross-border transfers, data residency, international access, international support operations, global vendor processing, international cloud services, and international privacy obligations applicable to information processed by Cognera Health™.

As a cloud-based healthcare technology organization, Cognera Health may utilize geographically distributed infrastructure, cloud providers, security services, backup

environments, disaster recovery environments, analytics platforms, artificial intelligence services, and support personnel located in different jurisdictions.

The organization recognizes that international data transfers create unique privacy, security, legal, contractual, operational, and regulatory obligations requiring enhanced governance and oversight.

This section establishes the controls, safeguards, accountability mechanisms, monitoring activities, and governance requirements supporting lawful and secure international information processing.

20.2 Policy Statement

Cognera Health shall implement governance controls designed to ensure that international processing and cross-border transfers are:

- Lawful
- Secure
- Transparent
- Documented
- Auditable
- Accountable
- Risk-Assessed
- Properly Governed

International processing activities shall support:

- Privacy Protection
- Security Protection
- Regulatory Compliance
- Data Protection
- Customer Requirements
- Contractual Requirements
- Information Governance Requirements

Information shall not be transferred internationally without appropriate safeguards and governance review where required.

20.3 International Processing Governance Objectives

The International Data Protection Program seeks to:

Protect Information
Protect information regardless of processing location.

Support Regulatory Compliance
Support applicable international privacy requirements.

Support Customer Requirements
Respect customer data residency and contractual obligations.

Support Operational Resilience
Enable geographically distributed operations while maintaining privacy protections.

Reduce Risk
Reduce:

- Privacy Risk
- Security Risk
- Regulatory Risk
- Operational Risk
- Vendor Risk

Maintain Trust
Promote confidence in international processing activities.

20.4 International Processing Scope

This section applies to:

- Cloud Infrastructure
- Backup Systems
- Disaster Recovery Systems
- Vendor Services
- AI Services
- Security Services
- Analytics Platforms
- Monitoring Systems
- Support Activities

- Administrative Activities
- Cross-Border Access
- International Data Transfers

20.5 Data Residency Governance

Policy Statement

Cognera Health shall respect applicable data residency, localization, sovereignty, customer, contractual, and regulatory requirements.

Governance Objectives

Support:

- Customer Requirements
- Regulatory Requirements
- Privacy Requirements
- Security Requirements
- Operational Requirements

Data Residency Reviews

Prior to significant processing activities, Cognera Health may evaluate:

- Storage Locations
- Processing Locations
- Backup Locations
- Vendor Locations
- Access Locations
- Regulatory Requirements

20.6 Cross-Border Data Transfer Governance

Policy Statement

Cross-border transfers shall occur only where appropriate safeguards exist.

Examples

Transfers may involve:

- Cloud Processing
- Vendor Services
- Analytics Services
- AI Services
- Security Services
- Disaster Recovery Activities

Governance Requirements

Transfers shall support:

- Privacy Reviews
- Security Reviews
- Risk Assessments
- Contract Reviews
- Customer Requirements

20.7 International Privacy Principles

All international processing activities shall support:

- Transparency
- Accountability
- Data Minimization
- Purpose Limitation
- Security Protection
- Privacy Protection
- Auditability
- Regulatory Compliance

20.8 International Data Categories

Information potentially subject to international processing may include:

- Personal Information
- Consumer Health Data
- PHI
- ePHI

- Behavioral Health Information
- Wellness Information
- Voice Information
- AI Information
- Operational Information
- Security Information

Enhanced Protections
Sensitive information shall receive enhanced protections during international processing.

20.9 International Cloud Processing Governance

Policy Statement

Cloud-based processing activities shall support privacy, security, compliance, and data protection requirements regardless of geographic location.

Governance Requirements

Examples include:

- Encryption
- Access Controls
- Logging
- Monitoring
- Backup Controls
- Disaster Recovery Controls

Cloud Reviews

Cloud environments shall be subject to:

- Security Reviews
- Privacy Reviews
- Risk Assessments
- Vendor Reviews

20.10 International Vendor Governance

Policy Statement

International vendors shall undergo enhanced governance review.

Review Activities

Examples include:

- Privacy Reviews
- Security Reviews
- Compliance Reviews
- Contract Reviews
- Risk Assessments
- Data Protection Reviews

Vendor Requirements

Examples include:

- Privacy Controls
- Security Controls
- Monitoring
- Incident Reporting
- Audit Support

20.11 International Artificial Intelligence Governance

Policy Statement

AI-enabled international processing activities require enhanced governance.

Examples

- AI Inference Services
- AI Analytics Services
- NLP Services
- Voice Processing Services
- Machine Learning Services

Governance Requirements

Examples include:

- Privacy Reviews

- Security Reviews
- AI Governance Reviews
- Vendor Reviews
- Risk Assessments

Restrictions

AI-related international processing shall not occur without appropriate governance review.

20.12 International Support Operations

Policy Statement

Support personnel located in different jurisdictions may access information only were authorized and necessary.

Examples

- Technical Support
- Infrastructure Support
- Security Operations
- Monitoring Activities
- Incident Response

Controls

Examples include:

- Least Privilege
- Need-to-Know
- Logging
- Monitoring
- Session Controls

20.13 International Access Governance

Policy Statement

International access shall be restricted and monitored.

Controls

Examples include:

- RBAC
- MFA
- Conditional Access
- Logging
- Monitoring
- Session Recording

Access Reviews

International access shall be reviewed periodically.

20.14 International Security Requirements

International processing activities shall support:

- Encryption
- Access Controls
- Logging
- Monitoring
- Incident Response
- Disaster Recovery
- Vulnerability Management
- Security Auditing

20.15 International Risk Management

Policy Statement

International processing activities shall undergo risk assessment.

Risk Categories

Examples include:

- Regulatory Risks
- Privacy Risks
- Security Risks
- Vendor Risks

- Geopolitical Risks
- AI Risks
- Data Residency Risks

Risk Mitigation Activities

Examples include:

- Assessments
- Reviews
- Monitoring
- Contractual Controls
- Security Controls

20.16 International Incident Management

Policy Statement

International incidents shall be managed according to established incident response procedures.

Examples

- Unauthorized Access
- Unauthorized Disclosure
- Vendor Incidents
- Cross-Border Compliance Issues
- AI Incidents

Response Activities

Examples include:

- Investigation
- Containment
- Remediation
- Notification
- Governance Review

20.17 International Documentation Requirements

Documentation may include:

- Processing Locations
- Transfer Activities
- Vendor Locations
- Risk Assessments
- Reviews
- Access Activities
- Compliance Reviews

Retention
Documentation shall be retained according to approved retention schedules.

20.18 Monitoring Program

Monitoring activities may include:

- International Access Monitoring
- Vendor Monitoring
- AI Monitoring
- Security Monitoring
- Transfer Monitoring

Objectives

Identify:

- Unauthorized Transfers
- Unauthorized Access
- Compliance Issues
- Governance Gaps

20.19 Auditing Program

Audits may include:

- Privacy Audits
- Security Audits

- Vendor Audits
- AI Audits
- International Processing Audits

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Risk Exposure
- Control Effectiveness

20.20 International Processing Metrics

Examples include:

- Transfer Reviews
- Vendor Reviews
- International Access Reviews
- Audit Findings
- Compliance Findings
- Security Findings
- AI Findings

20.21 Roles and Responsibilities

Privacy Officer

Responsible for:

- International Privacy Oversight
- Cross-Border Governance
- Privacy Reviews

Compliance Officer

Responsible for:

- Regulatory Monitoring

- Compliance Reviews

CISO

Responsible for:

- International Security Oversight
- Security Controls

Legal Counsel

Responsible for:

- Contract Reviews
- Regulatory Interpretation
- International Legal Requirements

Steering Committee

Responsible for:

- Governance Oversight
- High-Risk Reviews

20.22 Continuous Improvement

The International Data Protection Program shall be periodically reviewed to improve:

- Privacy Protection
- Security Protection
- Regulatory Readiness
- Vendor Governance
- AI Governance
- Risk Management
- Global Operations Governance

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes

- Following Significant Business Changes

The objective is to maintain a mature, secure, privacy-conscious, auditable, and enterprise-grade International Data Protection Program supporting all global processing activities throughout the Cognera Health ecosystem.

21. Data Retention, Deletion, Secure Disposal, Information Lifecycle Governance, Records Management, and Preservation Program

21.1 Purpose

Purpose Statement

The purpose of this section is to establish the governance framework governing the retention, preservation, archival, storage, protection, deletion, destruction, de-identification, anonymization, secure disposal, and lifecycle management of information processed by Cognera Health™.

Information retention and disposal activities are critical privacy, security, compliance, operational, legal, healthcare, and governance functions.

Improper retention may increase:

- Privacy Risk
- Security Risk
- Regulatory Risk
- Litigation Risk
- Operational Risk

Improper deletion may create:

- Compliance Failures
- Legal Exposure
- Continuity-of-Care Risks
- Audit Failures
- Regulatory Violations

This section establishes enterprise governance requirements ensuring that information is retained only as long as necessary and disposed of securely when no longer required.

21.2 Policy Statement

Cognera Health shall maintain a comprehensive Information Lifecycle Management Program governing the retention, archival, preservation, deletion, destruction, de-identification, anonymization, and secure disposal of information.

Information shall be retained only for legitimate:

- Clinical Purposes
- Healthcare Purposes
- Operational Purposes
- Security Purposes
- Compliance Purposes
- Regulatory Purposes
- Legal Purposes
- Contractual Purposes
- Continuity-of-Care Purposes
- Business Purposes

Information shall not be retained longer than necessary unless retention is required by law, regulation, contract, legal hold, investigation, audit, litigation, customer requirements, or other authorized preservation obligations.

21.3 Relationship to Data Retention Policy

Policy Statement

This Privacy Policy & Data Protection Program shall be read together with the:

Data Retention, Deletion, and Secure Disposal Policy

The Data Retention Policy remains the authoritative source governing:

- Retention Schedules
- Retention Periods
- Secure Disposal Standards
- Preservation Requirements

- Destruction Requirements
- Backup Retention Requirements

This section establishes governance requirements supporting those operational controls.

21.4 Information Lifecycle Governance

Policy Statement

All information shall be governed throughout its lifecycle.

Lifecycle Stages

Collection
Acquisition of information.

Creation
Generation of information.

Processing
Authorized use of information.

Storage
Maintenance in approved environments.

Access
Authorized retrieval.

Sharing
Authorized transfers.

Disclosure
Authorized releases.

Archival
Long-term preservation.

Retention
Maintenance according to approved schedules.

Deletion
Removal when eligible.

Destruction
Secure disposal.

Final Disposition
Completion of lifecycle activities.

21.5 Retention Governance Principles

All retention activities shall support:

- Data Minimization
- Storage Limitation
- Accountability
- Regulatory Compliance
- Continuity of Care
- Security Protection
- Risk Reduction
- Auditability

21.6 Records Management Program

Policy Statement

Cognera Health shall maintain a Records Management Program governing information maintained throughout the organization.

Objectives

Support:

- Regulatory Compliance
- Operational Efficiency
- Audit Readiness
- Legal Readiness
- Information Governance
- Privacy Protection

Record Categories

Examples include:

- Clinical Records
- Assessment Records
- Consent Records
- Audit Records
- Security Records
- Governance Records
- Vendor Records
- AI Records
- Voice Records

21.7 Information Subject to Retention Requirements

Examples include:

Clinical Documentation

- Progress Notes
- SOAP Notes
- Treatment Plans
- Care Plans

Assessment Information

- PHQ-9
- GAD-7
- OQ-45.2
- C-SSRS

Communications

- Messages
- Care Coordination Records
- Follow-Up Records

Consent Records

- HIPAA Authorizations
- AI Consents

- Voice Consents
- Telehealth Consents

Governance Records

- Policies
- Procedures
- Reviews
- Risk Assessments

Security Records

- Audit Logs
- Authentication Logs
- Incident Records

AI Records

- Inputs
- Outputs
- Validation Records
- Monitoring Records

Voice Records

- Audio Files
- Transcriptions
- Metadata

21.8 Data Minimization and Storage Limitation

Policy Statement

Information shall not be retained solely because storage capacity exists.

Objectives

Reduce:

- Privacy Risk
- Security Risk
- Regulatory Risk

- Operational Risk

Requirements

Retention must be supported by:

- Business Need
- Legal Obligation
- Regulatory Obligation
- Customer Requirement
- Security Requirement
- Continuity-of-Care Requirement

21.9 Archival Governance

Policy Statement

Certain information may require archival rather than deletion.

Examples

- Clinical Records
- Legal Records
- Audit Records
- Compliance Records
- Historical Governance Records

Archival Controls

Examples include:

- Encryption
- Access Controls
- Monitoring
- Retention Controls
- Disposal Controls

21.10 Legal Hold Governance

Policy Statement

Deletion and destruction activities shall be suspended when preservation obligations exist.

Trigger Events

Examples include:

- Litigation
- Regulatory Investigations
- OCR Investigations
- Security Investigations
- Government Requests
- Internal Investigations
- Contract Disputes
- Legal Reviews

Legal Hold Activities

Examples include:

- Hold Notices
- Custodian Identification
- System Identification
- Preservation Actions
- Monitoring

Release Requirements
Legal holds may be released only by authorized personnel.

21.11 Deletion Governance

Policy Statement

Information may be deleted only when:

- Retention requirements are satisfied.
- No legal hold exists.
- No preservation requirement exists.
- No regulatory restriction exists.

Authorized Deletion Triggers

Examples include:

- Retention Expiration
- Customer Offboarding
- Approved Rights Requests
- Contract Termination
- System Retirement
- Regulatory Authorization

Governance Requirements

Deletion activities shall support:

- Verification
- Documentation
- Auditability
- Monitoring

21.12 Privacy Rights and Deletion Requests

Policy Statement

Individuals may request deletion where legally permissible.

Evaluation Requirements

Requests shall be evaluated against:

- Retention Requirements
- Legal Obligations
- Regulatory Requirements
- Security Requirements
- Continuity-of-Care Requirements
- Investigations

Exceptions

Deletion may be denied where retention remains required.

21.13 De-Identification Governance

Policy Statement

Information may be de-identified where appropriate and legally permissible.

Purposes

Examples include:

- Analytics
- Reporting
- Product Improvement
- AI Development
- Research
- Quality Improvement

Governance Requirements

Examples include:

- Privacy Reviews
- Validation
- Monitoring
- Auditability

21.14 Anonymization Governance

Policy Statement

Information may be anonymized where appropriate.

Objectives

Support:

- Privacy Protection
- Research
- Analytics
- Risk Reduction

Controls

Examples include:

- Documentation
- Governance Reviews
- Validation

21.15 Secure Disposal Governance

Policy Statement

Information shall be securely disposed of when no longer required.

Objectives

Prevent:

- Unauthorized Access
- Unauthorized Recovery
- Reconstruction
- Disclosure

Disposal Activities

Examples include:

- Secure Deletion
- Cryptographic Erasure
- Secure Overwrite
- Media Sanitization
- Key Destruction
- Shredding
- Pulverization
- Certified Destruction

Standards Alignment

Examples include:

- NIST SP 800-88
- HIPAA Requirements

- Data Retention Policy

21.16 Backup Retention Governance

Policy Statement

Backup retention activities shall support:

- Disaster Recovery
- Business Continuity
- Security Operations
- Compliance Requirements

Backup Controls

Examples include:

Encryption

- Access Controls
- Monitoring
- Retention Controls
- Disposal Controls

21.17 Vendor Retention Governance

Policy Statement

Vendors shall support retention and disposal requirements.

Requirements

Examples include:

- Retention Controls
- Deletion Controls
- Secure Disposal Controls
- Destruction Verification
- Attestations

Verification Activities

Examples include:

- Reviews
- Certifications
- Audits
- Attestations

21.18 Monitoring Program

Monitoring activities may include:

- Retention Reviews
- Deletion Reviews
- Legal Hold Reviews
- Vendor Reviews
- Disposal Reviews

Objectives

Identify:

- Noncompliance
- Over-Retention
- Disposal Failures
- Governance Gaps

21.19 Auditing Program

Audits may include:

- Retention Audits
- Disposal Audits
- Legal Hold Audits
- Privacy Audits
- Security Audits
- Vendor Audits

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Control Effectiveness
- Risk Exposure

21.20 Retention Metrics

Examples include:

- Retention Compliance
- Deletion Compliance
- Disposal Compliance
- Legal Hold Compliance
- Vendor Compliance
- Audit Findings

21.21 Roles and Responsibilities

Privacy Officer

Responsible for:

- Privacy Retention Governance
- Rights Request Oversight
- Disposal Oversight

Compliance Officer

Responsible for:

- Compliance Monitoring
- Audit Coordination

Legal Counsel

Responsible for:

- Legal Holds
- Preservation Requirements

- Litigation Support

Data Owners

Responsible for:

- Retention Reviews
- Disposal Approval
- Governance Activities

Security Leadership

Responsible for:

- Secure Disposal Controls
- Destruction Verification

21.22 Continuous Improvement

The Information Lifecycle Management Program shall be periodically reviewed to improve:

- Privacy Protection
- Security Protection
- Regulatory Readiness
- Governance Maturity
- Operational Efficiency
- Retention Compliance

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Significant Business Changes

The objective is to maintain a mature, auditable, privacy-conscious, secure, and enterprise-grade Information Lifecycle Management Program supporting all information assets throughout the Cognera Health ecosystem.

22. Security Safeguards, Cybersecurity Governance, Information Protection Program, Security Operations, and Enterprise Security Management Framework

22.1 Purpose

Purpose Statement

The purpose of this section is to establish the enterprise cybersecurity, information security, privacy protection, operational security, cloud security, application security, artificial intelligence security, vendor security, and resilience governance requirements governing all information assets, systems, technologies, services, platforms, personnel, vendors, and operational activities throughout the Cognera Health™ ecosystem.

Information security serves as a foundational component of privacy governance.

Privacy protections cannot be effectively maintained without appropriate safeguards supporting the confidentiality, integrity, availability, authenticity, resilience, and recoverability of information.

This section establishes the governance framework through which information security controls are designed, implemented, monitored, tested, validated, audited, maintained, and continuously improved.

22.2 Policy Statement

Cognera Health shall maintain a comprehensive Information Security Program designed to protect information, systems, technologies, applications, services, networks, cloud environments, artificial intelligence systems, voice systems, and operational infrastructure from:

- Unauthorized Access
- Unauthorized Disclosure
- Unauthorized Modification
- Unauthorized Destruction
- Unauthorized Processing
- Theft
- Misuse

- Corruption
- Loss
- Service Disruption
- Cyberattack

Security activities shall support:

- Privacy Protection
- Regulatory Compliance
- Operational Resilience
- Customer Trust
- Business Continuity
- Responsible AI Governance

22.3 Security Governance Objectives

The Security Program seeks to:

Protect Confidentiality
Prevent unauthorized disclosure of information.

Protect Integrity
Prevent unauthorized modification of information.

Protect Availability
Ensure information and services remain available when needed.

Protect Privacy
Support privacy governance objectives.

Reduce Risk
Reduce:

- Security Risk
- Privacy Risk
- Regulatory Risk
- Operational Risk
- Vendor Risk
- AI Risk

Support Regulatory Compliance
Support healthcare, privacy, and cybersecurity obligations.

Support Business Continuity
Enable resilient and recoverable operations.

22.4 Security Governance Framework

The Security Governance Program consists of:

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards
- Operational Safeguards
- Cloud Security
- Application Security
- API Security
- Identity Governance
- Access Governance
- AI Security
- Voice Security
- Vendor Security
- Security Monitoring
- Incident Response
- Disaster Recovery
- Business Continuity

22.5 Security Governance Structure

Executive Leadership

Responsible for:

- Strategic Security Oversight
- Resource Allocation
- Enterprise Risk Oversight

CISO

Responsible for:

- Security Governance
- Security Operations
- Security Risk Management
- Security Monitoring

Privacy Officer

Responsible for:

- Security Support of Privacy Objectives
- Privacy-Security Coordination

Compliance Officer

Responsible for:

- Regulatory Readiness
- Security Compliance Reviews

Legal Counsel

Responsible for:

- Legal Risk Support
- Regulatory Interpretation

Data Governance Steering Committee

Responsible for:

- Security Governance Oversight
- Enterprise Risk Oversight

22.6 Administrative Safeguards

Policy Statement

Administrative safeguards establish governance, oversight, accountability, policies, procedures, training, and management controls supporting information protection.

Governance Activities

Examples include:

- Security Policies
- Security Standards
- Security Procedures
- Security Reviews
- Risk Assessments
- Vendor Reviews
- Governance Reporting

Administrative Objectives

Support:

- Accountability
- Oversight
- Risk Management
- Compliance
- Continuous Improvement

22.7 Security Risk Management Program

Policy Statement

Cognera Health shall maintain a Security Risk Management Program.

Risk Assessment Activities

Examples include:

- Enterprise Risk Assessments
- Vulnerability Assessments
- Threat Assessments
- Vendor Risk Assessments
- AI Risk Assessments
- Cloud Risk Assessments

Risk Categories

Examples include:

- Cybersecurity Risks

- Insider Risks
- Vendor Risks
- AI Risks
- Operational Risks
- Regulatory Risks

Risk Treatment

Examples include:

- Mitigation
- Acceptance
- Transfer
- Avoidance

22.8 Workforce Security Program

Policy Statement

Workforce members play a critical role in protecting information.

Workforce Security Activities

Examples include:

- Onboarding Controls
- Background Reviews
- Access Management
- Training
- Awareness Activities
- Termination Procedures

Workforce Responsibilities

Examples include:

- Protect Information
- Follow Policies
- Report Incidents
- Complete Training

22.9 Security Awareness and Training

Policy Statement

All workforce members shall complete security awareness training.

Training Topics

Examples include:

- HIPAA Security
- Privacy Awareness
- Password Security
- Phishing Awareness
- Social Engineering
- Incident Reporting
- AI Security
- Vendor Security

Frequency

Training shall occur:

- Upon Hire
- Annually
- Following Significant Changes
- Following Significant Incidents

22.10 Identity and Access Management (IAM)

Policy Statement

Access to information shall be restricted to authorized users.

IAM Objectives

Support:

- Least Privilege
- Need-to-Know
- Accountability
- Auditability

IAM Controls

Examples include:

- RBAC
- MFA
- SSO
- Conditional Access
- Session Controls
- Access Reviews

22.11 Authentication Governance

Authentication controls may include:

- Usernames
- Passwords
- MFA
- Security Keys
- Authenticator Applications
- Federated Identity Services

Authentication Objectives

Prevent:

- Unauthorized Access
- Credential Misuse
- Account Compromise

22.12 Authorization Governance

Authorization activities determine what resources users may access.

Authorization Models

Examples include:

- RBAC
- Least Privilege

- Need-to-Know
- Segregation of Duties

Review Activities
Authorization reviews shall occur periodically.

22.13 Encryption Program

Policy Statement

Sensitive information shall be protected using appropriate encryption controls.

Data at Rest

Examples include:

- Databases
- Storage Systems
- Backups
- Archives

Data in Transit

Examples include:

- TLS
- VPN Connections
- Secure APIs
- Secure Messaging

Key Management

Examples include:

- Key Rotation
- Key Storage
- Key Monitoring
- Key Protection

22.14 Application Security Program

Policy Statement

Applications shall be designed, developed, tested, deployed, and maintained according to secure development principles.

Covered Applications

Examples include:

- HealScript™
- HealConnect™
- APIs

Security Activities

Examples include:

- Secure Coding
- Code Reviews
- Security Testing
- Vulnerability Testing
- Penetration Testing

22.15 API Security Program

Policy Statement

APIs require enhanced governance due to their role in information exchange.

Controls

Examples include:

- Authentication
- Authorization
- Encryption
- Rate Limiting
- Monitoring
- Logging

Governance Objectives

Support:

- Security

- Privacy
- Availability
- Auditability

22.16 Cloud Security Program

Policy Statement

Cloud environments shall support security, privacy, resilience, and compliance requirements.

Cloud Controls

Examples include:

- Encryption
- Access Controls
- Monitoring
- Logging
- Backup Controls
- Recovery Controls
- Configuration Management

Cloud Governance Activities

Examples include:

- Security Reviews
- Risk Assessments
- Compliance Reviews
- Vendor Reviews

22.17 Security Logging and Audit Trails

Policy Statement

Security-relevant activities shall be logged.

Examples

- Authentication Events

- Access Events
- Administrative Activities
- Configuration Changes
- API Activities
- AI Activities
- Security Events

Governance Objectives

Support:

- Accountability
- Monitoring
- Investigations
- Compliance

22.18 Security Monitoring Program

Policy Statement

Cognera Health shall maintain security monitoring capabilities.

Monitoring Activities

Examples include:

- Access Monitoring
- Threat Monitoring
- SIEM Monitoring
- API Monitoring
- Cloud Monitoring
- AI Monitoring
- Voice Monitoring

Monitoring Objectives

Support:

- Threat Detection
- Incident Detection

- Risk Identification
- Compliance Monitoring

22.19 Vulnerability Management Program

Policy Statement

Vulnerabilities shall be identified, assessed, prioritized, remediated, and monitored.

Activities

Examples include:

- Vulnerability Scanning
- Configuration Reviews
- Security Assessments
- Patch Reviews

Prioritization Factors

Examples include:

- Severity
- Risk
- Exposure
- Business Impact

22.20 Patch Management Program

Policy Statement

Security patches shall be managed according to risk and operational requirements.

Activities

Examples include:

- Evaluation
- Testing
- Deployment
- Validation
- Monitoring

22.21 Artificial Intelligence Security

Policy Statement

AI systems require enhanced security governance.

Threat Categories

Examples include:

- Prompt Injection
- Model Manipulation
- Data Leakage
- Unauthorized Access
- Output Abuse
- Training Data Exposure

Controls

Examples include:

- Access Controls
- Monitoring
- Logging
- Validation
- Security Reviews

22.22 Voice and Audio Security

Policy Statement

Voice and audio information require enhanced security protections.

Controls

Examples include:

- Encryption
- Access Controls
- Logging
- Monitoring
- Retention Controls

- Disposal Controls

22.23 Vendor Security Governance

Policy Statement

Vendors shall maintain security controls appropriate to the information processed.

Vendor Requirements

Examples include:

- Security Assessments
- Risk Reviews
- Incident Reporting
- Access Controls
- Secure Disposal

Vendor Monitoring

Examples include:

- Security Reviews
- Compliance Reviews
- Risk Reviews

22.24 Business Continuity and Disaster Recovery

Policy Statement

Cognera Health shall maintain business continuity and disaster recovery capabilities.

Objectives

Support:

- Availability
- Recoverability
- Resilience
- Continuity of Operations

Activities

Examples include:

- Backups
- Recovery Testing
- Disaster Recovery Exercises
- Continuity Planning

22.25 Security Auditing Program

Security Audits

Examples include:

- Internal Audits
- External Assessments
- Vulnerability Assessments
- Penetration Tests
- AI Security Audits
- Cloud Security Audits

Audit Objectives

Evaluate:

- Security Controls
- Compliance
- Governance Effectiveness
- Risk Exposure

22.26 Security Metrics

Examples include:

- Security Incidents
- Vulnerabilities
- Patch Compliance
- Access Review Completion
- Vendor Security Findings
- AI Security Findings

- Audit Findings

Reporting

Reports may be provided to:

- CISO
- Privacy Officer
- Compliance Officer
- Executive Leadership
- Steering Committee

22.27 Security Exceptions Program

Policy Statement

Security exceptions shall be documented, approved, monitored, and periodically reviewed.

Requirements

Security exceptions shall include:

- Business Justification
- Risk Assessment
- Compensating Controls
- Expiration Date
- Approval Documentation

22.28 Roles and Responsibilities

CISO

Responsible for:

- Security Governance
- Security Operations
- Risk Management
- Incident Response

Privacy Officer
Responsible for:

- Privacy-Security Coordination
- Security Support of Privacy Controls

Compliance Officer
Responsible for:

- Security Compliance Monitoring
- Regulatory Readiness

Workforce Members

Responsible for:

- Following Policies
- Protecting Information
- Reporting Concerns
-

22.29 Continuous Improvement

The Security Program shall be periodically reviewed to improve:

- Confidentiality
- Integrity
- Availability
- Privacy Protection
- Security Protection
- Operational Resilience
- Governance Maturity

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Significant Technology Changes

The objective is to maintain a mature, resilient, auditable, secure, privacy-conscious, and enterprise-grade Security Governance Program supporting all information assets, technologies, services, and operations throughout the Cognera Health ecosystem.

23. Privacy Incident Response, Security Incident Response, Breach Management, Crisis Management, and Regulatory Notification Program

23.1 Purpose

Purpose Statement

The purpose of this section is to establish the enterprise governance framework governing the identification, reporting, classification, investigation, containment, remediation, escalation, documentation, notification, monitoring, recovery, and continuous improvement of privacy incidents, security incidents, breaches, cybersecurity events, artificial intelligence incidents, vendor incidents, and other events affecting the confidentiality, integrity, availability, privacy, security, or lawful processing of information.

Cognera Health™ recognizes that incidents are not solely technology events. Incidents may arise from:

- Human Error
- Process Failures
- Technology Failures
- Vendor Activities
- AI Activities
- Regulatory Issues
- Unauthorized Access
- Unauthorized Disclosure
- Operational Failures

This program is intended to ensure incidents are managed consistently, rapidly, effectively, transparently, and in accordance with applicable legal, regulatory, contractual, customer, and governance obligations.

23.2 Policy Statement

Cognera Health shall maintain a formal Privacy and Security Incident Response Program designed to:

- Detect Incidents
- Report Incidents
- Investigate Incidents
- Contain Incidents
- Remediate Incidents
- Document Incidents
- Escalate Incidents
- Notify Appropriate Parties
- Support Recovery Activities
- Improve Organizational Resilience

All workforce members, vendors, contractors, Business Associates, subcontractors, and authorized users shall promptly report suspected privacy or security incidents.

Failure to report incidents may result in increased organizational risk, regulatory exposure, customer harm, and compliance violations.

23.3 Incident Response Objectives

The Incident Response Program seeks to:

Protect Individuals
Reduce privacy harm and security impacts affecting individuals.

Protect Customers
Support customer obligations and operational continuity.

Protect Information
Reduce unauthorized access, disclosure, modification, or destruction.

Support Regulatory Compliance
Support applicable breach notification and incident response obligations.

Support Business Continuity
Minimize operational disruption.

Improve Organizational Resilience
Strengthen privacy and security capabilities.

Support Continuous Improvement
Incorporate lessons learned into governance and operational activities.

23.4 Incident Governance Principles

All incident response activities shall support:

- Accountability
- Timeliness
- Documentation
- Transparency
- Auditability
- Regulatory Compliance
- Risk Management
- Continuous Improvement

23.5 Incident Categories

Incidents may include:

- Privacy Incidents
- Security Incidents
- Cybersecurity Incidents
- Data Breaches
- AI Incidents
- Vendor Incidents
- Voice Processing Incidents
- Insider Threat Incidents
- Regulatory Incidents
- Business Continuity Events

23.6 Privacy Incident Definition

Definition

A privacy incident is an actual or suspected event involving unauthorized access, use, disclosure, sharing, exposure, modification, processing, loss, destruction, or misuse of information.

Examples

- Unauthorized Disclosure
- Misdirected Communications
- Excessive Sharing
- Improper Access
- Unauthorized AI Processing
- Unauthorized Recording
- Unauthorized Data Export
- Privacy Rights Failures

23.7 Security Incident Definition

Definition

A security incident is an actual or suspected event affecting the confidentiality, integrity, availability, security, resilience, or operation of systems or information.

Examples

- Unauthorized Access
- Malware
- Ransomware
- Account Compromise
- Credential Theft
- Network Intrusion
- Denial of Service
- Data Exfiltration

23.8 Breach Definition

Definition

A breach is an impermissible use, disclosure, acquisition, exposure, loss, alteration, or compromise of information meeting applicable legal, regulatory, contractual, or customer notification criteria.

Examples

- PHI Breaches
- ePHI Breaches
- Consumer Health Data Breaches
- Sensitive Information Breaches
- Vendor Breaches

23.9 Incident Severity Classification

Critical

Examples:

- Large-scale breach
- Significant ransomware attack
- Regulatory notification event
- Major AI failure affecting operations

Immediate Executive Escalation Required.

High

Examples:

- Unauthorized disclosure of sensitive information
- Significant vendor incident
- Material privacy incident

Executive Review Required.

Moderate

Examples:

- Limited disclosure
- Contained security event
- Isolated processing issue

Management Review Required.

Low

Examples:

- Minor policy violations
- Low-risk operational issues

Routine Management Required.

23.10 Incident Identification

Incidents may be identified through:

- Workforce Reporting
- Customer Reporting
- Vendor Reporting
- Monitoring Systems
- SIEM Alerts
- AI Monitoring
- Audits
- Security Reviews
- Privacy Reviews

23.11 Incident Reporting Requirements

Policy Statement

All workforce members shall promptly report suspected incidents.

Reportable Events

Examples include:

- Unauthorized Access
- Unauthorized Disclosure

- Lost Devices
- Malware
- Suspicious Activity
- Vendor Incidents
- AI Incidents
- Voice Processing Incidents

Reporting Channels

Examples include:

- Privacy Officer
- Compliance Officer
- Security Team
- Incident Response Team
- Executive Leadership

23.12 Incident Intake and Triage

Objectives

Determine:

- Severity
- Scope
- Impact
- Regulatory Implications
- Notification Requirements

Triage Activities

Examples include:

- Preliminary Investigation
- Impact Assessment
- Risk Assessment
- Escalation Review

23.13 Incident Investigation Program

Policy Statement

Significant incidents shall undergo formal investigation.

Investigation Activities

Examples include:

- Evidence Collection
- Timeline Reconstruction
- Impact Analysis
- Root Cause Analysis
- Risk Evaluation
- Exposure Assessment

Participants

May include:

- Privacy Officer
- Compliance Officer
- CISO
- Legal Counsel
- Vendor Representatives
- Executive Leadership

23.14 Incident Containment

Objectives

Prevent:

- Additional Exposure
- Additional Damage
- Additional Compromise
- Additional Data Loss

Containment Activities

Examples include:

- Access Restrictions
- Account Suspension
- Credential Resets
- Network Isolation
- Service Restrictions
- Vendor Coordination

23.15 Incident Remediation

Objectives

Correct identified issues and reduce recurrence.

Examples

- Security Improvements
- Process Improvements
- Additional Monitoring
- Policy Updates
- Training
- Vendor Remediation

23.16 HIPAA Breach Management

Policy Statement

Cognera Health shall support HIPAA Breach Notification Rule obligations where applicable.

Activities

Examples include:

- Breach Evaluation
- Risk Assessment
- Notification Support
- Documentation
- Corrective Actions

Governance Requirements

Examples include:

- Legal Review
- Privacy Review
- Compliance Review

23.17 Regulatory Notification Governance

Policy Statement

Where required by law, notifications shall be provided to appropriate regulatory authorities.

Examples

- OCR
- HHS
- State Regulators
- Privacy Regulators
- Government Authorities

Governance Requirements
Notifications shall undergo appropriate review before submission.

23.18 Customer Notification Governance

Policy Statement

Customers shall be notified according to contractual and regulatory requirements.

Examples

- Privacy Incidents
- Security Incidents
- Vendor Incidents
- AI Incidents
- Breaches

Objectives

Support:

- Transparency
- Coordination
- Compliance

23.19 Vendor Incident Governance

Policy Statement

Vendors shall report applicable incidents according to contractual obligations.

Vendor Responsibilities

Examples include:

- Reporting
- Investigation Support
- Remediation
- Corrective Actions
- Evidence Preservation

23.20 Artificial Intelligence Incident Governance

Examples

- Hallucinations
- Bias Findings
- Model Failures
- Privacy Violations
- Security Events
- Inaccurate Outputs

Governance Activities

Examples include:

- Investigation
- Validation
- Monitoring
- Governance Review

23.21 Voice and Recording Incident Governance

Examples

- Unauthorized Recording
- Unauthorized Disclosure
- Improper Transcription
- Voice Data Exposure
- Recording Consent Failures

Controls

Examples include:

- Investigation
- Documentation
- Monitoring
- Corrective Actions

23.22 Digital Forensics and Evidence Preservation

Policy Statement

Evidence associated with significant incidents shall be preserved appropriately.

Examples

- Audit Logs
- Authentication Logs
- Security Logs
- System Records
- Communications
- Vendor Records

Objectives

Support:

- Investigations
- Litigation

- Regulatory Reviews
- Root Cause Analysis

23.23 Crisis Management

Policy Statement

Certain incidents may require activation of crisis management procedures.

Examples

- Major Breaches
- Ransomware
- Widespread Service Disruption
- Significant Vendor Failure
- Public Safety Concerns

Participants

May include:

- Executive Leadership
- Privacy Officer
- Compliance Officer
- CISO
- Legal Counsel
- Communications Personnel

23.24 Incident Documentation

Incident records may include:

- Incident Identifier
- Incident Description
- Timeline
- Severity
- Impact
- Investigation Findings
- Root Cause
- Corrective Actions

- Notification Activities

Retention

Incident records shall be retained according to approved retention schedules.

23.25 Lessons Learned Program

Following significant incidents, Cognera Health shall evaluate:

- Root Causes
- Control Failures
- Governance Gaps
- Training Gaps
- Improvement Opportunities

Outputs

Examples include:

- Policy Updates
- Procedure Updates
- Technology Enhancements
- Additional Monitoring
- Additional Training

23.26 Incident Monitoring Program

Monitoring activities may include:

- Incident Trends
- Response Times
- Escalation Activities
- Vendor Incidents
- AI Incidents
- Breach Activities

Objectives

Identify:

- Emerging Risks
- Recurring Issues
- Process Weaknesses
- Governance Gaps

23.27 Incident Auditing Program

Audits may include:

- Incident Response Audits
- Breach Reviews
- Vendor Incident Audits
- AI Incident Audits
- Regulatory Notification Reviews

Audit Objectives

Evaluate:

- Compliance
- Timeliness
- Governance Effectiveness
- Control Effectiveness

23.28 Incident Metrics

Examples include:

- Privacy Incidents
- Security Incidents
- Breaches
- Vendor Incidents
- AI Incidents
- Mean Time to Detect
- Mean Time to Contain
- Mean Time to Resolve
- Audit Findings

23.29 Roles and Responsibilities

Privacy Officer

Responsible for:

- Privacy Incident Governance
- Breach Reviews
- Privacy Notifications

Compliance Officer

Responsible for:

- Compliance Monitoring
- Regulatory Coordination

CISO

Responsible for:

- Security Incident Governance
- Security Operations
- Incident Response

Legal Counsel

Responsible for:

- Legal Review
- Regulatory Guidance
- Litigation Support

Executive Leadership

Responsible for:

- Strategic Oversight
- Crisis Management
- Enterprise Escalation

23.30 Continuous Improvement

The Incident Response Program shall be periodically reviewed to improve:

- Privacy Protection
- Security Protection
- Detection Capabilities
- Response Capabilities
- Regulatory Readiness
- Governance Maturity

Reviews may occur:

- Following Significant Incidents
- Following Audits
- Following Regulatory Changes
- Following Technology Changes
- At Least Annually

The objective is to maintain a mature, resilient, auditable, and enterprise-grade Incident Response and Breach Management Program supporting all privacy, security, AI, voice, vendor, and operational incidents throughout the Cognera Health ecosystem.

24. Vendor Governance, Business Associate Governance, Third-Party Risk Management, Supply Chain Security, and External Service Provider Oversight Program

24.1 Purpose

Purpose Statement

The purpose of this section is to establish the governance framework governing the selection, onboarding, approval, management, monitoring, oversight, auditing, offboarding, and risk management of vendors, Business Associates, subcontractors, Cloud Service Providers (CSPs), Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), Artificial Intelligence providers, consultants, contractors, integration

partners, and other third parties that access, process, store, transmit, manage, support, or otherwise interact with information on behalf of Cognera Health™.

Third-party relationships represent one of the most significant sources of privacy, security, compliance, operational, and regulatory risk.

The organization recognizes that information entrusted to third parties remains subject to the same privacy, security, compliance, retention, governance, and accountability obligations that apply internally.

This section establishes a comprehensive Third-Party Governance Program designed to ensure that external service providers operate in a manner consistent with Cognera Health's privacy, security, compliance, AI governance, and information governance requirements.

24.2 Policy Statement

Cognera Health shall maintain a formal Vendor Governance and Third-Party Risk Management Program governing all external entities that access, process, transmit, store, manage, support, host, analyze, monitor, or otherwise interact with information or systems on behalf of the organization.

Third-party relationships shall be:

- Evaluated
- Risk Assessed
- Approved
- Contractually Governed
- Monitored
- Audited
- Documented
- Periodically Reviewed

No vendor shall be granted access to information or systems without appropriate governance review and authorization.

24.3 Program Objectives

The Vendor Governance Program seeks to:

Protect Information
Protect information entrusted to third parties.

Reduce Risk
Reduce:

- Privacy Risk
- Security Risk
- Vendor Risk
- Regulatory Risk
- Operational Risk
- AI Risk
- Supply Chain Risk

Support Compliance
Support applicable legal, regulatory, contractual, and customer obligations.

Improve Accountability
Ensure third parties remain accountable for information protection.

Support Operational Resilience
Promote continuity and reliability of services.

Maintain Trust
Promote confidence among customers, regulators, providers, and business partners.

24.4 Third-Party Governance Principles

All third-party relationships shall support:

- Accountability
- Transparency
- Risk Management
- Security Protection
- Privacy Protection
- Regulatory Compliance
- Auditability
- Continuous Monitoring
- Responsible AI Governance

24.5 Vendor Classification Framework

Policy Statement

All vendors shall be classified according to risk and business impact.

Critical Vendors

Examples include:

- Cloud Hosting Providers
- Infrastructure Providers
- Core Application Providers
- Security Providers
- AI Providers Supporting Core Services

High-Risk Vendors

Examples include:

- Vendors Processing PHI
- Vendors Processing Consumer Health Data
- Vendors Processing Behavioral Health Data
- Vendors Processing AI Data

Moderate-Risk Vendors

Examples include:

- Reporting Providers
- Analytics Providers
- Communications Providers

Low-Risk Vendors

Examples include:

- Administrative Service Providers
- General Business Service Providers

Governance Requirements

Higher-risk vendors require enhanced governance.

24.6 Vendor Due Diligence Program

Policy Statement

Vendors shall undergo due diligence before onboarding.

Due Diligence Areas

Examples include:

- Privacy Controls
- Security Controls
- Compliance Controls
- Risk Management
- Incident Response
- Business Continuity
- Disaster Recovery
- AI Governance
- Financial Stability
- Operational Maturity

Due Diligence Documentation

Examples include:

- Risk Assessments
- Security Reviews
- Privacy Reviews
- Vendor Questionnaires
- Compliance Reviews

24.7 Privacy Review Requirements

Policy Statement

Vendors processing sensitive information shall undergo privacy review.

Review Areas

Examples include:

- Data Collection
- Data Processing
- Data Sharing
- Data Retention
- Data Disposal
- Privacy Rights Support
- Consent Support

Privacy Approval Requirements
Privacy approval may be required before onboarding.

24.8 Security Review Requirements

Policy Statement

Vendors shall undergo security review appropriate to their risk profile.

Review Areas

Examples include:

- Access Controls
- Encryption
- Logging
- Monitoring
- Incident Response
- Vulnerability Management
- Secure Development
- Security Governance

Security Documentation

Examples include:

- Security Assessments
- Penetration Testing Results
- Security Certifications

- Risk Assessments

24.9 Business Associate Governance

Policy Statement

Business Associates shall be governed through enhanced controls due to their access to PHI and ePHI.

Business Associate Requirements

Examples include:

- Business Associate Agreements
- Privacy Controls
- Security Controls
- Incident Reporting
- Audit Support
- Retention Controls
- Secure Disposal

Business Associate Monitoring
Business Associates shall be monitored periodically.

24.10 Data Processing Agreement Governance

Policy Statement

Where required, Data Processing Agreements (DPAs) shall be executed.

DPA Areas

Examples include:

- Processing Activities
- Privacy Obligations
- Security Obligations
- Data Subject Rights
- Retention Requirements
- Incident Reporting

24.11 Artificial Intelligence Vendor Governance

Policy Statement

AI vendors require enhanced governance due to the unique risks associated with AI processing.

Review Areas

Examples include:

- AI Security
- AI Privacy
- AI Governance
- AI Transparency
- AI Explainability
- AI Risk Management
- AI Monitoring

Restrictions
AI vendors shall not receive information without appropriate governance approval.

24.12 Cloud Service Provider Governance

Policy Statement

Cloud providers require enhanced oversight due to their role in hosting and processing information.

Review Areas

Examples include:

- Security Controls
- Privacy Controls
- Infrastructure Resilience
- Disaster Recovery
- Data Residency
- Regulatory Compliance

Monitoring Requirements

Cloud providers shall undergo periodic review.

24.13 MSP and MSSP Governance

MSP Governance

Managed Service Providers shall support:

- Operational Security
- Privacy Protection
- Incident Response
- Governance Requirements

MSSP Governance

Managed Security Service Providers shall support:

- Threat Monitoring
- Incident Detection
- Security Operations
- Investigation Support

24.14 Vendor Access Governance

Policy Statement

Vendor access shall be restricted according to business need.

- Access Principles
- Least Privilege
- Need-to-Know
- Time-Limited Access
- Role-Based Access

Controls

Examples include:

- MFA
- Logging

- Monitoring
- Access Reviews

24.15 Third-Party Risk Management

Policy Statement

Vendor risks shall be evaluated throughout the vendor lifecycle.

Risk Categories

Examples include:

- Privacy Risks
- Security Risks
- Regulatory Risks
- Operational Risks
- AI Risks
- Financial Risks
- Reputational Risks

Risk Mitigation Activities

Examples include:

- Reviews
- Monitoring
- Corrective Actions
- Audits
- Contractual Controls

24.16 Vendor Monitoring Program

Policy Statement

Vendors shall be monitored throughout the relationship lifecycle.

Monitoring Activities

Examples include:

- Security Monitoring

- Compliance Monitoring
- Privacy Monitoring
- Incident Monitoring
- Performance Monitoring
- AI Monitoring

Objectives

Identify:

- Control Failures
- Compliance Issues
- Security Concerns
- Operational Risks

24.17 Vendor Audit Program

Policy Statement

Vendors may be subject to audits and governance reviews.

Audit Areas

Examples include:

- Privacy Controls
- Security Controls
- Compliance Controls
- AI Governance
- Retention Controls
- Disposal Controls

Audit Objectives

Evaluate:

- Compliance
- Governance Effectiveness
- Risk Exposure

- Contractual Compliance

24.18 Vendor Incident Management

Policy Statement

Vendors shall report incidents according to contractual obligations.

Examples

- Privacy Incidents
- Security Incidents
- Data Breaches
- AI Incidents
- Service Disruptions

Vendor Responsibilities

Examples include:

- Reporting
- Investigation Support
- Remediation
- Corrective Actions
- Evidence Preservation

24.19 Vendor Performance Management

Objectives

Evaluate:

- Service Quality
- Security Performance
- Privacy Performance
- Compliance Performance
- Incident Performance

Reviews

Vendor performance reviews may occur periodically.

24.20 Vendor Offboarding Program

Policy Statement

Vendor relationships shall undergo controlled offboarding.

Offboarding Activities

Examples include:

- Access Revocation
- Data Return
- Data Deletion
- Secure Disposal
- Contract Closure
- Documentation Updates

Verification Activities

Examples include:

- Destruction Certificates
- Attestations
- Reviews
- Audit Evidence

24.21 Supply Chain Security Governance

Policy Statement

Supply chain risks shall be incorporated into governance activities.

Risk Areas

Examples include:

- Fourth-Party Risks
- AI Supply Chain Risks
- Cloud Dependency Risks

- Infrastructure Risks
- Operational Risks

Controls

Examples include:

- Risk Assessments
- Monitoring
- Reviews
- Escalation Procedures

24.22 Vendor Documentation Requirements

Documentation may include:

- Risk Assessments
- Privacy Reviews
- Security Reviews
- Contracts
- BAAs
- DPAs
- Audit Reports
- Monitoring Records

Retention
Vendor governance records shall be retained according to approved retention schedules.

24.23 Vendor Metrics

Examples include:

- Vendor Risk Scores
- Vendor Audit Findings
- Vendor Incidents
- Vendor Compliance Rates
- Vendor Review Completion Rates
- AI Vendor Findings

- Offboarding Completion Rates

24.24 Roles and Responsibilities

Privacy Officer

Responsible for:

- Privacy Reviews
- Vendor Privacy Oversight

Compliance Officer

Responsible for:

- Compliance Reviews
- Regulatory Oversight

CISO

Responsible for:

- Security Reviews
- Vendor Security Oversight

Legal Counsel

Responsible for:

- Contracts
- BAAs
- DPAs
- Legal Risk Reviews

Steering Committee

Responsible for:

- High-Risk Vendor Approvals
- Governance Oversight

24.25 Continuous Improvement

The Vendor Governance Program shall be periodically reviewed to improve:

- Privacy Protection
- Security Protection
- Vendor Accountability
- AI Governance
- Supply Chain Security
- Compliance Readiness
- Governance Maturity

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Significant Vendor Changes

The objective is to maintain a mature, auditable, secure, privacy-conscious, resilient, and enterprise-grade Vendor Governance and Third-Party Risk Management Program supporting all external relationships throughout the Cognera Health ecosystem.

25. Privacy Complaints, Escalation Management, Regulatory Inquiry Response, Ethics Reporting, and Privacy Dispute Resolution Program

25.1 Purpose

Purpose Statement

The purpose of this section is to establish a comprehensive Privacy Complaints and Escalation Management Program governing the receipt, review, investigation, resolution, documentation, monitoring, reporting, escalation, and continuous improvement of privacy-related concerns, complaints, allegations, inquiries, disputes, and regulatory matters.

Cognera Health™ recognizes that effective complaint management is an essential component of privacy governance, transparency, accountability, trust, and regulatory compliance.

Complaints provide valuable insight into potential weaknesses in privacy controls, security controls, consent practices, information handling activities, vendor activities, artificial intelligence governance, and operational processes.

This program is intended to ensure that concerns are addressed fairly, objectively, consistently, transparently, and in accordance with applicable legal, regulatory, contractual, and organizational requirements.

25.2 Policy Statement

Cognera Health shall maintain a formal Privacy Complaints and Escalation Program designed to:

- Receive Complaints
- Document Complaints
- Investigate Complaints
- Resolve Complaints
- Escalate Complaints
- Monitor Trends
- Report Findings
- Improve Governance

All complaints shall be reviewed objectively and without retaliation against the reporting individual.

The organization shall maintain reasonable procedures supporting privacy-related inquiries, complaints, appeals, ethics concerns, whistleblower concerns, and regulatory inquiries.

25.3 Program Objectives

The Privacy Complaints Program seeks to:

Protect Individuals
Address privacy concerns affecting individuals.

Support Transparency
Provide mechanisms for reporting concerns.

Support Accountability
Ensure concerns are documented and addressed.

Support Regulatory Compliance
Support complaint handling obligations.

Improve Governance
Identify opportunities for improvement.

Reduce Risk
Reduce:

- Privacy Risk
- Security Risk
- Regulatory Risk
- Operational Risk
- Reputational Risk

25.4 Complaint Governance Principles

All complaint activities shall support:

- Fairness
- Objectivity
- Confidentiality
- Accountability
- Documentation
- Auditability
- Timeliness
- Non-Retaliation
- Continuous Improvement

25.5 Complaint Types

Examples include:

- Privacy Complaints
- Security Complaints
- Rights Request Complaints
- Consent Complaints
- AI Complaints
- Vendor Complaints
- Consumer Health Data Complaints
- Voice Processing Complaints
- Regulatory Complaints
- Ethical Concerns

25.6 Privacy Complaints

Examples include:

- Unauthorized Disclosure
- Unauthorized Access
- Excessive Collection
- Improper Sharing
- Improper Retention
- Deletion Failures
- Privacy Rights Concerns

25.7 Security Complaints

Examples include:

- Security Weaknesses
- Credential Issues
- Account Compromise
- Security Misconfigurations
- Access Control Concerns

25.8 Artificial Intelligence Complaints

Examples include:

- Bias Concerns
- Explainability Concerns
- AI Output Concerns
- Transparency Concerns
- Hallucinations
- Inappropriate Recommendations

25.9 Consumer Health Data Complaints

Examples include:

- Wellness Data Concerns
- Mood Tracking Concerns
- Consumer Rights Concerns
- Consent Concerns
- Sharing Concerns

25.10 Voice and Recording Complaints

Examples include:

- Unauthorized Recording
- Recording Consent Issues
- Voice Processing Concerns
- Transcription Issues
- Voice Privacy Concerns

25.11 Complaint Submission Channels

Complaints may be submitted through:

- Privacy Office
  - privacy@cogneraheath.ai
- Compliance Office
  - compliance@cogneraheath.ai
- Security Office

- security@cognerahealth.ai
- Customer Support
- Customer Administrators
- Authorized Representatives
- Written Correspondence
- Regulatory Referrals

25.12 Complaint Intake Process

All complaints shall:

- Receive Tracking Identifier
- Be Logged
- Be Categorized
- Be Assigned
- Be Tracked
- Be Monitored

Intake Documentation

Examples include:

- Complaint Number
- Date Received
- Source
- Category
- Severity
- Status
- Resolution

25.13 Complaint Severity Classification

Critical

Examples include:

- Major Privacy Breaches
- Significant Regulatory Matters

- Public Safety Concerns
- Executive Escalation Events

High

Examples include:

- Significant Privacy Issues
- High-Risk Security Issues
- High-Risk AI Issues

Moderate

Examples include:

- Isolated Processing Concerns
- Rights Request Issues
- Consent Issues

Low

Examples include:

- General Inquiries
- Minor Concerns
- Informational Requests

25.14 Complaint Investigation Program

Policy Statement

Complaints shall undergo appropriate investigation.

Investigation Activities

Examples include:

- Information Gathering
- Record Reviews
- Interviews
- Risk Assessment
- Root Cause Analysis
- Evidence Collection

Investigation Participants

May include:

- Privacy Officer
- Compliance Officer
- CISO
- Legal Counsel
- Product Leadership
- Operations Leadership

25.15 Escalation Management

Policy Statement

Certain complaints require escalation.

Escalation Triggers

Examples include:

- Regulatory Risk
- Significant Privacy Risk
- Significant Security Risk
- Litigation Risk
- Public Relations Risk
- Executive Risk

Escalation Levels

Level 1
Operational Review

Level 2
Management Review

Level 3
Privacy Officer Review

Level 4
Executive Leadership Review

Level 5
Steering Committee Review

25.16 Regulatory Inquiry Management

Policy Statement

Cognera Health shall maintain procedures supporting regulatory inquiries.

Examples

- OCR Inquiries

- HHS Inquiries
- State Regulator Inquiries
- Privacy Regulator Inquiries
- Consumer Protection Agency Inquiries

Activities

Examples include:

- Information Collection
- Investigation Support
- Response Preparation
- Corrective Actions

25.17 Ethics and Whistleblower Reporting

Policy Statement

Cognera Health supports reporting of concerns involving:

- Privacy
- Security
- Compliance
- Ethics
- Governance
- AI Activities
- Vendor Activities

Non-Retaliation
Individuals reporting concerns in good faith shall be protected from retaliation.

25.18 Corrective Action Program

Corrective actions may include:

- Policy Updates
- Procedure Updates
- Security Improvements

- Privacy Improvements
- Training
- Vendor Remediation
- AI Governance Improvements

25.19 Complaint Documentation Requirements

Records may include:

- Complaint Description
- Investigation Activities
- Findings
- Root Cause
- Corrective Actions
- Resolution
- Escalations

Retention
Complaint records shall be retained according to approved retention schedules.

25.20 Monitoring Program

Monitoring activities may include:

- Complaint Trends
- Escalation Trends
- Regulatory Inquiries
- Rights Complaints
- AI Complaints
- Vendor Complaints

Objectives

Identify:

- Emerging Risks
- Control Failures
- Process Weaknesses
- Governance Gaps

25.21 Auditing Program

Audits may include:

- Complaint Handling Audits
- Escalation Audits
- Regulatory Inquiry Reviews
- Corrective Action Reviews

Audit Objectives

Evaluate:

- Timeliness
- Consistency
- Documentation Quality
- Governance Effectiveness

25.22 Complaint Metrics

Examples include:

- Complaint Volume
- Complaint Categories
- Resolution Time
- Escalation Rate
- Regulatory Inquiries
- Repeat Issues
- Corrective Action Completion

25.23 Roles and Responsibilities

Privacy Officer

Responsible for:

- Privacy Complaints
- Escalations

- Reporting

Compliance Officer

Responsible for:

- Regulatory Inquiries
- Compliance Reviews

CISO

Responsible for:

- Security Complaints
- Security Escalations

Legal Counsel

Responsible for:

- Legal Matters
- Litigation Support
- Regulatory Responses

Executive Leadership

Responsible for:

- Strategic Oversight
- High-Risk Escalations

25.24 Continuous Improvement

The Privacy Complaints Program shall be periodically reviewed to improve:

- Transparency
- Responsiveness
- Governance Maturity
- Customer Trust
- Regulatory Readiness

The objective is to maintain a fair, transparent, auditable, accountable, and enterprise-grade Privacy Complaints and Escalation Program supporting all privacy governance activities throughout the Cognera Health ecosystem.

26. Privacy Office Structure, Contact Information, Governance Functions, Organizational Reporting Structure, and Privacy Program Administration

26.1 Purpose

Purpose Statement

The purpose of this section is to establish the organizational structure, responsibilities, authority, reporting relationships, contact mechanisms, operational functions, and governance activities supporting the Cognera Health™ Privacy Office and Privacy Program Administration.

The Privacy Office serves as the central authority responsible for coordinating privacy governance, privacy operations, privacy compliance, privacy risk management, privacy rights administration, privacy investigations, privacy reporting, privacy monitoring, and privacy program oversight.

The Privacy Office functions as an enterprise governance capability designed to support organizational accountability, regulatory readiness, customer trust, information protection, and responsible information management.

This section defines how privacy governance is operationalized across the organization and establishes clear pathways for communication, escalation, reporting, inquiries, complaints, and governance coordination.

26.2 Policy Statement

Cognera Health shall maintain a formal Privacy Office responsible for the administration, coordination, oversight, monitoring, and continuous improvement of the Privacy & Data Protection Program.

The Privacy Office shall:

- Coordinate Privacy Governance
- Support Regulatory Compliance
- Support Privacy Rights
- Support Privacy Investigations
- Support Risk Management
- Support AI Governance
- Support Vendor Governance
- Support Information Governance
- Support Incident Response

The Privacy Office shall operate with sufficient authority, independence, visibility, and organizational support to perform its responsibilities effectively.

26.3 Privacy Office Mission

The mission of the Privacy Office is to:

- Protect privacy.
- Promote accountability.
- Support transparency.
- Support compliance.
- Reduce risk.
- Enable responsible innovation.
- Maintain trust.
- Foster governance maturity.

The Privacy Office seeks to ensure privacy remains integrated into organizational decision-making, technology development, operational activities, and customer-facing services.

26.4 Privacy Office Objectives

The Privacy Office seeks to:

Protect Information
Support protection of sensitive information.

Support Privacy Rights
Administer privacy rights requests.

Support Regulatory Readiness
Prepare for audits, reviews, and investigations.

Support Privacy Governance
Coordinate governance activities.

Support Risk Management
Identify and mitigate privacy risks.

Support Responsible AI
Coordinate privacy oversight of AI systems.

Support Vendor Governance
Review third-party privacy risks.

Support Continuous Improvement
Improve privacy maturity across the organization.

26.5 Privacy Office Structure

The Privacy Office may consist of multiple governance functions depending upon organizational size, maturity, operational complexity, regulatory obligations, and business requirements.

Privacy Officer

The Privacy Officer serves as the primary authority responsible for privacy governance.

Responsibilities

Examples include:

- Privacy Governance
- Privacy Program Administration
- Privacy Risk Management
- Privacy Rights Administration
- Privacy Reporting
- Privacy Reviews
- Privacy Escalations

Privacy Operations

Responsible for:

- Rights Requests
- Consent Management
- Complaint Administration
- Documentation Management
- Privacy Reviews

Privacy Compliance

Responsible for:

- Regulatory Monitoring
- Audit Coordination
- Compliance Reviews
- Corrective Actions

Privacy Risk Management

Responsible for:

- Privacy Assessments
- DPIAs
- PIAs
- Risk Reviews
- Risk Reporting

Privacy Investigations

Responsible for:

- Privacy Incidents
- Breach Reviews
- Complaint Investigations
- Regulatory Support

26.6 Organizational Reporting Structure

Executive Leadership

Provides:

- Strategic Oversight
- Governance Sponsorship
- Resource Allocation

Data Governance Steering Committee

Provides:

- Governance Oversight
- Policy Approval
- Risk Oversight

Privacy Officer

Reports privacy program status to:

- Executive Leadership
- Steering Committee
- Compliance Leadership

Cross-Functional Governance

The Privacy Office coordinates with:

- Security
- Compliance
- Legal
- Product
- Engineering
- Operations
- Customer Success
- Clinical Advisors
- AI Governance Teams

26.7 Privacy Office Functions

The Privacy Office shall support the following functions.

Privacy Governance

Examples include:

- Policy Development
- Standards Development
- Governance Reviews
- Governance Reporting

Privacy Rights Administration

Examples include:

- Access Requests
- Deletion Requests
- Correction Requests
- Appeals
- Complaints

Privacy Risk Management

Examples include:

- Privacy Assessments
- Risk Reviews
- Governance Reviews

Incident Management Support

Examples include:

- Privacy Investigations
- Breach Reviews
- Regulatory Notifications

Vendor Privacy Governance

Examples include:

- Vendor Reviews
- Privacy Assessments
- Vendor Monitoring

AI Privacy Governance

Examples include:

- AI Reviews
- AI Risk Assessments
- AI Monitoring

26.8 Privacy Office Contact Channels

Privacy Rights Requests

For requests involving:

- Access
- Correction
- Deletion
- Restriction
- Portability
- Objection

Contact: privacy@cogneraheath.ai

Privacy Complaints

For complaints involving:

- Privacy Concerns
- Disclosure Concerns
- Consent Concerns
- Consumer Health Data Concerns

Contact: privacy@cogneraheath.ai

Compliance Matters

For:

- Compliance Questions
- Regulatory Inquiries
- Governance Questions

Contact: compliance@cogneraheath.ai

Security Matters

For:

- Security Concerns
- Security Incidents
- Vulnerability Reporting

Contact: security@cogneraheath.ai

Legal Matters

For:

- Legal Requests
- Court Orders
- Subpoenas
- Litigation Matters

Contact: legal@cogneraheath.ai

General Inquiries

Contact: info@cogneraheath.ai

26.9 Privacy Office Communication Standards

Policy Statement

Privacy communications shall be:

- Professional
- Accurate
- Timely
- Respectful
- Documented
- Consistent

Communication Activities

Examples include:

- Rights Responses
- Complaint Responses
- Regulatory Responses
- Customer Communications

- Internal Communications

26.10 Privacy Program Reporting

Internal Reporting

Examples include:

- Privacy Metrics
- Risk Metrics
- Audit Findings
- Rights Metrics
- Vendor Findings
- AI Findings

Executive Reporting

Examples include:

- Strategic Risks
- Significant Incidents
- Governance Maturity
- Compliance Status

Governance Reporting

Examples include:

- Steering Committee Reports
- Risk Reports
- Audit Reports

26.11 Privacy Program Documentation Management

The Privacy Office shall maintain documentation supporting:

- Policies
- Procedures
- Standards
- Rights Requests

- Complaints
- Investigations
- Audits
- Risk Assessments
- Governance Reviews

Retention
Privacy program documentation shall be retained according to approved retention schedules.

26.12 Privacy Program Metrics

Examples include:

- Rights Requests
- Complaints
- Privacy Incidents
- Audit Findings
- Risk Assessments
- Vendor Reviews
- AI Reviews
- Training Completion

26.13 Privacy Program Escalation Framework

Matters requiring escalation may include:

- Major Privacy Incidents
- Regulatory Investigations
- Significant Privacy Risks
- High-Risk Vendor Findings
- High-Risk AI Findings
- Litigation Matters
- Customer Escalations

Escalation Authorities

Examples include:

- Privacy Officer
- Compliance Officer
- CISO
- Legal Counsel
- Executive Leadership
- Steering Committee

26.14 Privacy Office Independence

Policy Statement

The Privacy Office shall maintain sufficient independence to perform privacy oversight responsibilities objectively.

Privacy reviews, investigations, audits, and governance activities shall be conducted free from improper influence.

The Privacy Office shall have authority to:

- Escalate Risks
- Request Reviews
- Require Corrective Actions
- Recommend Governance Changes

26.15 Continuous Improvement

The Privacy Office shall periodically evaluate:

- Program Effectiveness
- Governance Maturity
- Regulatory Readiness
- Customer Expectations
- AI Governance Readiness
- Operational Efficiency

The objective is to maintain a mature, scalable, transparent, accountable, and enterprise-grade Privacy Office capable of supporting all privacy governance activities throughout the Cognera Health ecosystem.

27. Enterprise Glossary, Definitions, Terminology, Acronyms, and Governance Reference Dictionary

27.1 Purpose

Purpose Statement

The purpose of this glossary is to establish standardized definitions for privacy, security, healthcare, compliance, governance, artificial intelligence, records management, vendor governance, information governance, risk management, and operational terminology used throughout the Cognera Health™ Privacy & Data Protection Program.

Consistent terminology supports:

- Regulatory Compliance
- Governance Consistency
- Operational Clarity
- Risk Management
- Audit Readiness
- Customer Communication
- Vendor Communication
- Workforce Training

Unless otherwise defined by applicable law, regulation, contract, or policy, the definitions contained within this glossary shall govern the interpretation of this Privacy & Data Protection Program.

Term	Definition
Access Control	A security mechanism restricting access to information, systems, services, applications, or resources to authorized individuals.
Access Review	A formal review of user access rights to validate appropriateness and necessity.
Account Deprovisioning	Removal or disabling of user access when no longer authorized.
Account Provisioning	Process of creating, modifying, and removing user accounts.
Administrative Safeguards	Governance, policy, procedural, workforce, and management controls designed to protect information.

Term	Definition
Advanced Persistent Threat (APT)	A sophisticated and prolonged cyberattack conducted by a skilled threat actor.
AI (Artificial Intelligence)	Technology capable of generating outputs, predictions, recommendations, classifications, summaries, or insights using computational models and algorithms.
AI Accountability	Assignment of responsibility for AI system outcomes and governance.
AI Governance	The framework governing the design, development, deployment, operation, monitoring, validation, oversight, and retirement of AI systems.
AI Hallucination	AI-generated output that is inaccurate, fabricated, or unsupported by evidence.
AI Incident	An event involving an AI system that may create privacy, security, compliance, operational, ethical, or reputational risks.
AI Lifecycle	The stages of design, development, deployment, operation, monitoring, and retirement of AI systems.
AI Model	A machine learning, statistical, generative, predictive, or computational model used to produce outputs.
AI Monitoring	Ongoing oversight of AI performance, risks, outputs, and controls.
AI Oversight Committee	Governance body responsible for AI governance decisions.
AI Risk Assessment	Structured evaluation of privacy, security, operational, ethical, legal, compliance, and reputational risks associated with AI systems.
AI Safety	Measures designed to prevent harmful AI outcomes.
AI Transparency	Ability to understand AI system purpose, functionality, limitations, and governance.
AI Validation	Process used to confirm AI systems meet intended objectives and requirements.
AI Vendor	Third-party organization providing AI technologies, models, infrastructure, APIs, services, or capabilities.
Algorithmic Transparency	Ability to understand and explain how an AI system produces outputs.

Term	Definition
Anonymization	Irreversible removal of identifying information such that an individual cannot reasonably be identified.
API (Application Programming Interface)	Technology enabling communication between software systems.
Asset Inventory	Documented record of organizational assets requiring governance and protection.
Asset Management	Processes used to identify, classify, maintain, protect, and manage assets.
Audit	Structured review evaluating compliance, governance, controls, effectiveness, or operational performance.
Audit Log	Chronological record of activities performed within a system, application, service, or environment.
Authentication	Process of verifying the identity of a user, device, service, or system.
Authorization	Process of determining what actions an authenticated user is permitted to perform.
Availability	Assurance that information and systems are accessible when needed.
BAA (Business Associate Agreement)	Contract governing the use, disclosure, protection, and management of PHI between a Covered Entity and a Business Associate.
Backup	Copy of information maintained for recovery purposes.
Behavioral Health Information	Information relating to emotional, behavioral, psychological, psychiatric, or substance-use health.
Bias	Systematic error or unfair outcome produced by data, models, processes, or decisions.
Biometric Identifier	Measurable biological characteristic used to identify an individual.
Biometric Information	Information derived from biometric identifiers used for identification, authentication, or verification.
BIPA	Illinois Biometric Information Privacy Act.
Breach	Impermissible use, disclosure, access, acquisition, exposure, loss, or compromise of information meeting notification requirements.

Term	Definition
Business Associate	Entity performing functions involving PHI on behalf of a Covered Entity.
Business Continuity	Ability to maintain critical operations during and after a disruption.
Business Impact Analysis (BIA)	Assessment identifying critical operations and recovery requirements.
Care Coordination	Activities supporting communication and collaboration among providers, care teams, organizations, and individuals.
CCPA	California Consumer Privacy Act.
Change Management	Controlled process for implementing modifications to systems, applications, infrastructure, or processes.
Chief Compliance Officer (CCO)	Executive responsible for compliance oversight.
Chief Information Security Officer (CISO)	Executive responsible for information security governance.
Clinical Documentation	Documentation supporting healthcare, behavioral health, wellness, or care activities.
Cloud Service Provider (CSP)	Organization providing cloud infrastructure, storage, platform, or application services.
Compliance Officer	Individual responsible for compliance governance and oversight.
Confidential Information	Information requiring protection from unauthorized access or disclosure but not classified as Restricted Information.
Configuration Management	Governance of system configurations to maintain security and operational consistency.
Consent	Freely given, informed, specific, and documented agreement permitting certain processing activities.
Consumer Health Data	Health-related information subject to consumer privacy protections and not necessarily governed by HIPAA.
Consumer Privacy Rights	Rights granted to individuals under privacy laws and regulations.
Continuous Monitoring	Ongoing assessment of controls, risks, threats, vulnerabilities, and compliance obligations.
Control	Safeguard designed to reduce risk or achieve compliance objectives.

Term	Definition
Corrective Action	Activity implemented to address identified deficiencies, issues, or nonconformities.
Covered Entity	Healthcare provider, health plan, or healthcare clearinghouse subject to HIPAA.
CPRA	California Privacy Rights Act.
Critical Risk	Risk level requiring executive review and immediate governance attention.
Cross-Border Transfer	Movement of information between countries or jurisdictions.
Cybersecurity	Protection of information systems, applications, networks, and data from threats.
Crisis Management	Coordination of organizational response during significant disruptions.
Data Classification	Categorization of information according to sensitivity and protection requirements.
Data Controller	Entity determining the purposes and means of processing information.
Data Governance	Framework governing information throughout its lifecycle.
Data Integrity	Assurance that information remains accurate, complete, and unaltered.
Data Lake	Centralized repository storing structured and unstructured information.
Data Mapping	Documentation of information flows and processing activities.
Data Minimization	Principle of collecting and processing only information reasonably necessary for an authorized purpose.
Data Owner	Individual or function accountable for governance of specific information assets.
Data Processor	Entity processing information on behalf of another entity.
Data Protection Impact Assessment (DPIA)	Structured assessment evaluating privacy risks associated with high-risk processing activities.
Data Residency	Requirements governing where information may be stored or processed.
Data Retention	Maintenance of information for a defined period.
Data Steward	Individual responsible for supporting governance and quality management of information assets.

Term	Definition
Data Subject	Individual whose personal information is processed.
Data Subject Request (DSR)	Request by an individual to exercise privacy rights.
De-Identification	Removal of identifying elements from information according to applicable standards.
Defense-in-Depth	Security strategy using multiple layers of protection.
Deletion	Removal of information according to approved retention and disposal requirements.
Designated Record Set	Records maintained by or for a covered entity used to make decisions about individuals.
Detection and Response	Activities designed to identify, investigate, contain, and respond to threats and incidents.
Differential Privacy	Technique used to protect privacy while enabling statistical analysis.
Disclosure	Release, transfer, provision, publication, or sharing of information to another party.
Disposal	Final destruction, deletion, sanitization, or disposition of information.
Disaster Recovery	Activities supporting restoration of technology services following disruption.
DPA (Data Processing Agreement)	Contract governing processing activities between organizations.
Due Diligence	Investigation and evaluation performed before decisions, engagements, or transactions.
eDiscovery	Identification, preservation, collection, and production of electronically stored information.
Emergency Response	Immediate actions taken during disruptive events.
Encryption	Conversion of information into a protected format requiring authorized decryption.
Endpoint	User device or system connected to organizational resources.
Endpoint Detection and Response (EDR)	Technology used to monitor and respond to endpoint threats.
Enterprise Risk Management	Framework used to identify, assess, monitor, and manage organizational risks.

Term	Definition
Ethics Committee	Governance body responsible for ethical oversight.
Ethics Review	Governance review evaluating fairness, responsibility, transparency, and ethical considerations.
Explainability	Ability to understand how AI systems generate outputs.
Fairness	Principle that systems and processes avoid unjustified bias, discrimination, or inequitable outcomes.
Federated Learning	Machine learning approach where models train across decentralized data sources.
Final Disposition	Completion of an information asset's lifecycle through deletion, destruction, or approved archival.
Firewall	Technology controlling network traffic based on security rules.
GDPR	General Data Protection Regulation.
Generative AI	AI capable of creating text, images, audio, video, code, or other content.
Governance	Structures, authorities, responsibilities, oversight activities, and controls directing organizational activities.
Governance Committee	Oversight group responsible for governance decisions and accountability.
HealConnect™	Cognera Health's engagement, wellness, behavioral health, communication, and continuous care platform.
HealScript™	Cognera Health's provider, practitioner, operational intelligence, and clinical workflow platform.
HHS	United States Department of Health and Human Services.
HIPAA	Health Insurance Portability and Accountability Act.
HITRUST	Health Information Trust Alliance.
HITECH	Health Information Technology for Economic and Clinical Health Act.
Human-in-the-Loop	Governance model requiring human review, validation, approval, modification, or override of AI outputs.
Identity Management	Processes governing user identities and access rights.
Identity Provider (IdP)	Service managing user authentication and identity information.
Incident	Event affecting privacy, security, compliance, confidentiality, integrity, or availability.

Term	Definition
Incident Response	Structured approach to managing and resolving incidents.
Information Asset	Any information, record, dataset, file, document, system, repository, or resource containing information.
Information Governance	Management of information throughout its lifecycle.
Information Security	Protection of confidentiality, integrity, and availability of information.
Integrity	Protection of information against unauthorized modification or corruption.
Large Language Model (LLM)	AI model trained on large datasets to understand and generate language.
Legal Hold	Suspension of deletion or destruction activities due to legal, regulatory, investigative, or litigation requirements.
Least Privilege	Principle of granting only the minimum access necessary to perform authorized activities.
Logging	Recording of activities occurring within systems, services, applications, or environments.
Machine Learning (ML)	Subset of AI enabling systems to learn patterns from data.
MFA	Multi-Factor Authentication.
Minimum Necessary	HIPAA principle limiting access, use, disclosure, and sharing to the minimum reasonably necessary amount.
Model Drift	Degradation of AI model performance over time.
Monitoring	Ongoing observation and review of activities, controls, systems, or information.
MSSP	Managed Security Service Provider.
MSP	Managed Service Provider.
Need-to-Know	Access principle restricting information access to those with a legitimate business requirement.
NIST	National Institute of Standards and Technology.
NLP	Natural Language Processing.
NLU	Natural Language Understanding.
OCR	Office for Civil Rights.
Operational Intelligence	Reporting, analytics, metrics, and insights supporting organizational operations.
Penetration Testing	Authorized testing designed to identify security weaknesses.

Term	Definition
Personal Information	Information identifying, relating to, describing, or reasonably capable of being associated with an individual.
PHI	Protected Health Information.
Privacy by Default	Limiting information processing to what is necessary by default.
Privacy by Design	Incorporation of privacy protections into systems and processes.
Privacy Impact Assessment (PIA)	Structured review evaluating privacy implications of processing activities.
Privacy Officer	Individual responsible for privacy governance and oversight.
Processing	Any operation performed on information including collection, use, storage, sharing, analysis, retention, deletion, or destruction.
Prompt	Instruction or input provided to an AI system.
Prompt Injection	Attempt to manipulate AI behavior through crafted instructions.
Pseudonymization	Processing information so it cannot be attributed to a specific individual without additional information.
Purpose Limitation	Principle that information shall be processed only for authorized and documented purposes.
RBAC	Role-Based Access Control.
Records Management	Governance of information throughout its lifecycle.
Recovery Point Objective (RPO)	Maximum acceptable amount of data loss measured in time.
Recovery Time Objective (RTO)	Maximum acceptable time to restore operations following disruption.
Recovery Testing	Validation of backup and recovery capabilities.
Regulatory Inquiry	Request, review, investigation, audit, or examination by a regulatory authority.
Responsible AI	Governance approach promoting safe, lawful, ethical, transparent, and trustworthy AI use.
Restricted Information	Highest sensitivity classification requiring enhanced protections.
Retention Schedule	Documented schedule specifying retention periods and disposition requirements.

Term	Definition
Retrieval-Augmented Generation (RAG)	AI architecture combining retrieval systems with generative models.
Right of Access	Right to obtain information regarding processing activities.
Right to Correction	Right to request correction of inaccurate information.
Right to Deletion	Right to request deletion of information under applicable law.
Right to Object	Right to object to specific processing activities.
Right to Portability	Right to receive information in a portable format.
Right to Restrict Processing	Right to limit processing activities under applicable law.
Risk Assessment	Structured evaluation of threats, vulnerabilities, impacts, and controls.
Risk Owner	Individual accountable for management of a specific risk.
Secure Disposal	Approved destruction methods preventing unauthorized recovery or reconstruction of information.
Security Awareness Training	Education designed to improve workforce security practices.
Security by Design	Integration of security requirements throughout system development.
Security Incident	Event involving unauthorized access, disclosure, modification, destruction, or disruption of information or systems.
Sensitive Personal Information	Personal information requiring enhanced protections due to sensitivity or regulatory requirements.
SIEM	Security Information and Event Management.
Single Sign-On (SSO)	Authentication process allowing access to multiple systems with one login.
Storage Limitation	Principle that information should not be retained longer than necessary.
Subcontractor	Third party engaged by another third party to perform services.
Synthetic Data	Artificially generated data used for training, testing, or analysis.
Telehealth	Healthcare services delivered through telecommunications technologies.

Term	Definition
Third Party	Any organization or individual outside Cognera Health with whom information may be shared.
Threat Actor	Individual or organization capable of causing harm.
Threat Intelligence	Information regarding threats, vulnerabilities, risks, and attack methods.
TLS	Transport Layer Security.
TPO	Treatment, Payment, and Healthcare Operations.
Unauthorized Access	Access occurring without appropriate authorization.
Unauthorized Disclosure	Release of information without proper authority.
User	Individual authorized to access systems, services, applications, or information.
Validation	Process of confirming outputs, controls, systems, or activities meet established requirements.
Vendor	Third-party organization providing services, products, software, infrastructure, support, or operational capabilities.
Voice-to-Text	Technology converting spoken audio into written text.
Vulnerability	Weakness that may be exploited to compromise confidentiality, integrity, or availability.
Vulnerability Assessment	Evaluation designed to identify weaknesses in systems, applications, or controls.
Washington My Health My Data Act	State privacy law governing consumer health data.
Workforce	Employees, contractors, temporary personnel, interns, volunteers, consultants, and other authorized individuals acting on behalf of Cognera Health.
Zero Trust	Security model based on continuous verification and least-privilege access.

27.2 Glossary Governance

The Enterprise Glossary shall be:

- Reviewed Annually
- Updated Following Regulatory Changes
- Updated Following Governance Changes

- Updated Following Significant Technology Changes

New definitions may be approved by:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Data Governance Steering Committee

to ensure consistency throughout the Cognera Health Privacy & Data Protection Program.

28. References, Legal Authorities, Regulatory Sources, Governance Standards, and Control Framework Alignment

28.1 Purpose

Purpose Statement

The purpose of this section is to identify the laws, regulations, standards, frameworks, guidance documents, governance sources, contractual authorities, and organizational policies that inform, support, and influence the Cognera Health™ Privacy & Data Protection Program.

This section serves as the authoritative reference framework supporting privacy governance, security governance, compliance governance, artificial intelligence governance, information governance, records management, risk management, and operational governance activities throughout the organization.

The references contained within this section are intended to support:

- Regulatory Alignment
- Governance Consistency
- Compliance Readiness
- Audit Readiness
- Customer Due Diligence
- Risk Management
- Program Development
- Continuous Improvement

28.2 Policy Statement

Cognera Health shall maintain awareness of applicable laws, regulations, frameworks, standards, industry guidance, contractual obligations, and governance expectations relevant to its operations.

References identified within this section shall be monitored periodically to determine whether updates to policies, procedures, controls, governance activities, training programs, or operational practices are necessary.

The references listed below are intended to inform governance activities and do not imply certification, accreditation, attestation, endorsement, approval, or regulatory determination unless expressly stated elsewhere.

28.3 Healthcare Regulatory References

HIPAA
Health Insurance Portability and Accountability Act of 1996

Examples include:

- **HIPAA Privacy Rule**
  - 45 CFR Part 160
  - 45 CFR Part 164 Subparts A and E
- **HIPAA Security Rule**
  - 45 CFR Part 160
  - 45 CFR Part 164 Subparts A and C
- **HIPAA Breach Notification Rule**
  - 45 CFR Part 164 Subpart D

HITECH Act
Health Information Technology for Economic and Clinical Health Act

Governance Areas:

- Breach Notification
- Security Controls
- Business Associate Requirements
- Enforcement Provisions

OCR Guidance
Office for Civil Rights guidance documents and enforcement guidance where applicable.

28.4 Privacy Law References

GDPR
General Data Protection Regulation (EU) 2016/679

Examples include:

- **Article 5**
  - Data Processing Principles
- **Article 6**
  - Lawful Basis
- **Article 9**
  - Special Category Data
- **Article 13**
  - Transparency Requirements
- **Article 15**
  - Right of Access
- **Article 16**
  - Right to Rectification
- **Article 17**
  - Right to Erasure
- **Article 18**
  - Restriction of Processing
- **Article 20**
  - Data Portability
- **Article 21**
  - Right to Object

UK GDPR
United Kingdom General Data Protection Regulation

CCPA
California Consumer Privacy Act

CPRA
California Privacy Rights Act

Consumer Health Data Laws

Examples include:

- Washington My Health My Data Act
- Applicable State Consumer Health Privacy Laws

State Privacy Laws

Examples include:

- Texas Data Privacy and Security Act
- Colorado Privacy Act
- Virginia Consumer Data Protection Act
- Connecticut Data Privacy Act
- Utah Consumer Privacy Act
- Emerging State Privacy Laws

Biometric Privacy Laws

Examples include:

- Illinois Biometric Information Privacy Act (BIPA)
- Applicable State Biometric Privacy Requirements

28.5 Cybersecurity References

NIST Cybersecurity Framework

Functions include:

- Identify
- Protect
- Detect
- Respond
- Recover

NIST SP 800-53
Security and Privacy Controls

NIST SP 800-66
HIPAA Security Rule Guidance

NIST SP 800-88
Media Sanitization and Secure Disposal Guidance

NIST AI Risk Management Framework
Guidance supporting AI governance and AI risk management activities.

28.6 Information Security Standards

ISO/IEC 27001
Information Security Management Systems

ISO/IEC 27002
Information Security Controls

ISO/IEC 27701
Privacy Information Management Systems

ISO/IEC 27017
Cloud Security Guidance

ISO/IEC 27018
Protection of Personal Information in Public Clouds

28.7 Healthcare and Risk Frameworks

HITRUST CSF

Healthcare-focused privacy, security, compliance, and risk management framework.

Risk Management Principles

Examples include:

- Enterprise Risk Management
- Privacy Risk Management
- Cybersecurity Risk Management
- Vendor Risk Management
- AI Risk Management

28.8 Artificial Intelligence Governance References

NIST AI RMF

AI Risk Management Framework

Responsible AI Principles

Examples include:

- Transparency
- Explainability
- Accountability
- Human Oversight
- Fairness
- Safety

Emerging AI Regulations

Examples include:

- State AI Laws
- International AI Governance Requirements
- Healthcare AI Guidance

28.9 Records Management References

Examples include:

- Information Lifecycle Management
- Records Retention Requirements
- Secure Disposal Standards
- Legal Hold Requirements
- eDiscovery Requirements

28.10 Internal Governance References

This Privacy & Data Protection Program shall be read together with:

- Compliance Governance Framework
- Data Retention, Deletion, and Secure Disposal Policy

- Artificial Intelligence Governance Program
- AI Consent Framework
- Information Security Program
- Incident Response Program
- Vendor Governance Program
- Business Continuity Program
- Disaster Recovery Program
- HealScript™ Governance Requirements
- HealConnect™ Governance Requirements
- CogneraAI™ Governance Requirements
- Privacy Notices
- Terms & Conditions
- EULA Documents

28.11 Customer and Contractual Authorities

Governance activities may also be influenced by:

- Customer Contracts
- Business Associate Agreements
- Data Processing Agreements
- Service Agreements
- Vendor Agreements
- Regulatory Requirements
- Customer Security Requirements
- Customer Privacy Requirements

28.12 Reference Governance

Policy Statement

References shall be reviewed periodically.

Review Triggers

Examples include:

- Regulatory Changes
- New Legislation

- Enforcement Actions
- Industry Guidance
- Customer Requirements
- Significant Incidents
- Governance Reviews

Responsibilities

Examples include:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- CISO
- Data Governance Steering Committee

28.13 Continuous Improvement

Reference sources shall be evaluated periodically to ensure that governance activities remain:

- Current
- Relevant
- Effective
- Compliant
- Risk-Aware
- Aligned with Industry Expectations

The objective is to maintain a governance framework informed by authoritative, relevant, and evolving legal, regulatory, privacy, security, healthcare, and artificial intelligence guidance sources.

29. Document Governance, Approval Authority, Version Control, Change Management, Review Cycles, and Program Administration

29.1 Purpose

Purpose Statement

The purpose of this section is to establish the governance framework governing the creation, approval, maintenance, distribution, review, modification, version control, retirement, and administration of the Cognera Health™ Privacy & Data Protection Program and all associated privacy governance documentation.

Document governance is essential to ensuring that policies remain:

- Current
- Accurate
- Consistent
- Authoritative
- Auditable
- Controlled
- Aligned with Regulatory Requirements
- Aligned with Organizational Objectives

This section establishes accountability and oversight mechanisms designed to ensure that privacy governance documentation remains effective and appropriately maintained throughout its lifecycle.

29.2 Policy Statement

Cognera Health shall maintain formal governance controls governing privacy program documentation.

All privacy governance documents shall:

- Have Assigned Ownership
- Have Defined Approval Authorities
- Have Defined Review Cycles

- Be Version Controlled
- Be Maintained in Approved Repositories
- Be Auditable
- Be Periodically Reviewed
- Be Updated as Necessary

Privacy governance documents shall not be modified, distributed, retired, superseded, or replaced without appropriate authorization.

29.3 Governance Objectives

The Document Governance Program seeks to:

Maintain Accuracy
Ensure documents remain accurate and current.

Maintain Regulatory Alignment
Ensure documents reflect applicable requirements.

Maintain Accountability
Ensure ownership is clearly assigned.

Support Audit Readiness
Maintain evidence of governance activities.

Support Operational Consistency
Promote consistent application of privacy requirements.

Support Continuous Improvement
Enable updates based on evolving risks and requirements.

29.4 Document Scope

This section applies to:

- Privacy Policies
- Privacy Standards
- Privacy Procedures
- Governance Frameworks
- AI Governance Documents

- Data Retention Policies
- Security Governance Documents
- Vendor Governance Documents
- Consent Frameworks
- EULA Documents
- Internal Governance Standards
- Supporting Documentation

29.5 Document Classification

Privacy governance documentation shall be classified according to sensitivity.

Restricted

Examples include:

- Risk Assessments
- Incident Reports
- Investigation Records
- Security Findings
- Internal Audit Findings

Confidential

Examples include:

- Internal Governance Policies
- Governance Procedures
- Compliance Documentation
- Vendor Assessments

Internal

Examples include:

- Training Materials
- Administrative Procedures
- Internal Communications

Public

Examples include:

- Public Privacy Notices
- Website Privacy Policies
- Public Trust Center Content

29.6 Document Ownership

Policy Statement

Every governance document shall have an assigned owner.

Responsibilities

Document Owners shall:

- Maintain Content
- Coordinate Reviews
- Coordinate Updates
- Maintain Accuracy
- Support Audits
- Ensure Regulatory Alignment
- Manage Version History

29.7 Document Approval Authority

Policy Statement

Governance documents shall be approved by designated authorities before becoming effective.

- Approval Authorities
- Privacy Officer

Approves:

- Privacy Policies
- Privacy Standards
- Privacy Procedures

Compliance Officer

Reviews:

- Compliance Requirements
- Regulatory Alignment

CISO

Reviews:

- Security Requirements
- Security Controls

Legal Counsel

Reviews:

- Legal Requirements
- Regulatory Obligations

Data Governance Steering Committee

Approves:

- Enterprise Governance Policies
- Enterprise Frameworks
- Retention Schedules
- AI Governance Policies

Executive Leadership
May ratify enterprise-level governance documents.

29.8 Document Lifecycle Management

Policy Statement

All governance documents shall be managed throughout their lifecycle.

Lifecycle Stages

- Creation
- Drafting

- Review
- Approval
- Publication
- Distribution
- Maintenance
- Revision
- Retirement
- Archival
- Disposal

29.9 Version Control Program

Policy Statement

All governance documentation shall be subject to formal version control.

Version Requirements

Documents shall include:

- Document Title
- Document Identifier
- Version Number
- Effective Date
- Review Date
- Approval Date
- Owner
- Classification

Version Numbering

Examples:

Major Versions

- 1.0
- 2.0
- 3.0

Minor Revisions

- 3.1
- 3.2
- 3.3

Version History

Document changes shall be recorded.

Examples include:

- Change Description
- Date
- Approver
- Version Number

29.10 Change Management Program

Policy Statement

Changes to governance documents shall be formally managed.

Change Triggers

Examples include:

- Regulatory Changes
- Audit Findings
- Incident Findings
- Risk Assessments
- Technology Changes
- Organizational Changes
- AI Governance Changes
- Vendor Governance Changes

Change Activities

Examples include:

- Review
- Impact Assessment
- Stakeholder Review

- Approval
- Documentation

29.11 Review Cycles

Policy Statement

Governance documentation shall undergo periodic review.

Minimum Review Frequency

At least annually unless otherwise specified.

Additional Review Triggers

Examples include:

- Regulatory Changes
- Major Incidents
- Security Events
- Privacy Events
- Significant Vendor Changes
- Significant AI Changes
- Organizational Restructuring

29.12 Distribution Management

Policy Statement

Governance documents shall be distributed appropriately.

Distribution Objectives

Ensure:

- Availability
- Version Consistency
- Access Control
- Accountability

Distribution Methods

Examples include:

- Governance Repositories
- Document Management Systems
- Internal Portals
- Training Platforms

29.13 Document Repository Governance

Policy Statement

Approved governance documentation shall be maintained in authorized repositories.

Repository Requirements

Examples include:

- Access Controls
- Version Control
- Audit Logging
- Backup Protection
- Recovery Capabilities

29.14 Document Retirement Program

Policy Statement

Superseded or obsolete documents shall be retired in a controlled manner.

Retirement Activities

Examples include:

- Archive Prior Versions
- Update References
- Remove Obsolete Copies
- Notify Stakeholders
- Preserve History

Retirement Approval

Document retirement shall require appropriate approval.

29.15 Audit and Compliance Support

Policy Statement

Document governance activities shall support audit readiness.

Audit Evidence

Examples include:

- Approval Records
- Review Records
- Version Histories
- Change Logs
- Distribution Records

Objectives

Demonstrate:

- Accountability
- Governance
- Compliance
- Continuous Improvement

29.16 Governance Reporting

Reports may include:

- Review Completion Rates
- Document Currency Status
- Outstanding Reviews
- Policy Exceptions
- Audit Findings
- Governance Metrics

Reporting Recipients

Examples include:

- Privacy Officer
- Compliance Officer
- CISO
- Steering Committee
- Executive Leadership

29.17 Exceptions Management

Policy Statement

Exceptions to document governance requirements shall be documented and approved.

Exception Requirements

Examples include:

- Business Justification
- Risk Assessment
- Compensating Controls
- Approval Documentation
- Expiration Date

29.18 Roles and Responsibilities

Privacy Officer

Responsible for:

- Privacy Documentation
- Privacy Governance Records
- Policy Maintenance

Compliance Officer

Responsible for:

- Regulatory Alignment Reviews
- Compliance Documentation

CISO

Responsible for:

- Security Governance Documentation
- Security Review Activities

Legal Counsel

Responsible for:

- Legal Reviews
- Regulatory Reviews

Steering Committee

Responsible for:

- Governance Approval
- Oversight
- Strategic Direction

29.19 Program Administration

The Privacy Program Administration function shall coordinate:

- Document Reviews
- Approvals
- Version Management
- Governance Reporting
- Audit Support
- Repository Management
- Change Tracking

29.20 Continuous Improvement

The Document Governance Program shall be periodically reviewed to improve:

- Governance Effectiveness
- Audit Readiness
- Regulatory Alignment
- Documentation Quality

- Accountability
- Operational Efficiency

Reviews may occur:

- Annually
- Following Audits
- Following Incidents
- Following Regulatory Changes
- Following Major Governance Changes

The objective is to maintain a mature, controlled, auditable, accountable, and enterprise-grade governance framework for all privacy program documentation throughout the Cognera Health ecosystem.

30. Privacy Program Conclusion, Strategic Commitment, Executive Statement, and Ongoing Governance Commitment

30.1 Executive Privacy Commitment

Cognera Health™ is committed to maintaining a comprehensive, mature, accountable, and continuously improving privacy, data protection, information governance, security, compliance, artificial intelligence governance, records management, and risk management program.

Privacy is a foundational component of the organization's mission, culture, operational philosophy, governance framework, and long-term strategy.

The organization recognizes that healthcare, behavioral health, wellness, consumer health, artificial intelligence, and digital health technologies require a heightened commitment to privacy, security, transparency, accountability, and responsible stewardship of information.

Cognera Health is committed to protecting the confidentiality, integrity, availability, lawful use, ethical management, and responsible governance of information entrusted to the organization by:

- Individuals
- Providers
- Practitioners

- Care Teams
- Healthcare Organizations
- Behavioral Health Organizations
- Wellness Organizations
- Customers
- Business Partners
- Regulatory Authorities

This commitment extends throughout the entire information lifecycle and applies to all technologies, products, services, personnel, vendors, contractors, and operational activities.

30.2 Privacy Philosophy

Cognera Health believes that privacy is more than a legal obligation.

Privacy is:

- A Trust Obligation
- A Governance Obligation
- A Security Obligation
- A Customer Commitment
- An Ethical Responsibility
- A Strategic Imperative

The organization recognizes that privacy failures may create significant impacts affecting:

- Individuals
- Healthcare Organizations
- Behavioral Health Organizations
- Customers
- Providers
- Care Teams
- Communities

Accordingly, privacy considerations shall remain integrated into organizational decision-making, product development, technology implementation, vendor management, artificial intelligence deployment, operational activities, and governance processes.

30.3 Enterprise Information Stewardship Commitment

Cognera Health acknowledges its responsibility as a steward of information entrusted to the organization.

The organization commits to:

Protect Information
Protect information from unauthorized access, disclosure, modification, destruction, loss, misuse, and compromise.

Use Information Responsibly
Use information only for authorized and appropriate purposes.

Minimize Information Collection
Collect only information reasonably necessary to support authorized purposes.

Maintain Transparency
Provide appropriate visibility into information practices.

Respect Individual Rights
Support privacy rights and consumer protections where applicable.

Maintain Accountability
Ensure information processing activities remain governed, monitored, and auditable.

Support Ethical Use
Promote fairness, responsibility, and ethical information management practices.

30.4 Privacy by Design Commitment

Cognera Health commits to incorporating privacy considerations into:

- Product Development
- Platform Design
- Software Development
- Artificial Intelligence Development
- Integrations
- Vendor Relationships
- Operational Processes

- Business Activities

Privacy shall be considered from the earliest stages of planning through retirement and disposal activities.

The organization seeks to proactively identify privacy risks rather than react to privacy failures.

30.5 Security by Design Commitment

Cognera Health recognizes that privacy cannot be effectively maintained without security.

The organization commits to implementing and maintaining administrative, technical, operational, organizational, and physical safeguards designed to support:

- Confidentiality
- Integrity
- Availability
- Resilience
- Recoverability
- Accountability

Security governance shall remain integrated with privacy governance and information governance activities.

30.6 Responsible Artificial Intelligence Commitment

Cognera Health recognizes the opportunities and risks associated with Artificial Intelligence.

The organization is committed to deploying AI technologies in a manner that is:

- Responsible
- Transparent
- Explainable
- Accountable
- Ethical
- Secure
- Privacy-Conscious

- Human-Governed

AI technologies shall support and augment human decision-making while preserving appropriate human oversight and accountability.

Cognera Health remains committed to maintaining governance mechanisms designed to evaluate, monitor, validate, audit, and continuously improve AI-enabled capabilities.

30.7 Regulatory Compliance Commitment

Cognera Health is committed to supporting applicable requirements arising from:

- HIPAA
- HITECH
- GDPR
- UK GDPR
- CCPA
- CPRA
- Consumer Health Data Laws
- State Privacy Laws
- Biometric Privacy Laws
- Healthcare Regulations
- Cybersecurity Requirements
- Contractual Obligations
- Customer Requirements

The organization recognizes that privacy and security requirements continue to evolve and therefore commits to maintaining ongoing regulatory monitoring and governance review activities.

30.8 Customer Trust Commitment

Trust is foundational to the Cognera Health mission.

The organization is committed to maintaining the trust of:

- Individuals
- Providers
- Practitioners

- Care Teams
- Healthcare Organizations
- Behavioral Health Organizations
- Wellness Organizations
- Customers
- Partners
- Regulators

Cognera Health recognizes that trust must be earned continuously through responsible actions, transparency, accountability, and consistent governance.

30.9 Governance Maturity Commitment

Cognera Health acknowledges that privacy governance is a continuous journey rather than a static destination.

The organization commits to:

- Ongoing Assessment
- Ongoing Monitoring
- Ongoing Auditing
- Ongoing Training
- Ongoing Risk Management
- Ongoing Program Improvement
- Ongoing Regulatory Monitoring
- Ongoing Technology Evaluation

The organization shall continuously evaluate opportunities to strengthen privacy, security, compliance, AI governance, information governance, and operational resilience.

30.10 Continuous Improvement Commitment

Cognera Health shall maintain a culture of continuous improvement.

Program enhancements may be driven by:

- Audit Findings
- Incident Findings
- Risk Assessments

- Regulatory Changes
- Customer Feedback
- Vendor Reviews
- AI Governance Reviews
- Security Reviews
- Industry Best Practices
- Governance Maturity Assessments

Continuous improvement activities shall seek to improve:

- Privacy Protection
- Security Protection
- Governance Effectiveness
- Regulatory Readiness
- Customer Confidence
- Operational Efficiency
- AI Governance Maturity

30.11 Executive Governance Statement

Executive Leadership affirms its commitment to supporting the Cognera Health Privacy & Data Protection Program through:

- Strategic Oversight
- Resource Allocation
- Governance Sponsorship
- Risk Management
- Regulatory Readiness
- Accountability
- Continuous Improvement

Privacy, security, compliance, information governance, artificial intelligence governance, and responsible stewardship of information remain strategic priorities of the organization.

30.12 Enterprise Program Statement

The Cognera Health™ Privacy & Data Protection Program serves as the authoritative enterprise governance framework governing privacy, data protection, information

governance, artificial intelligence governance, records management, consent management, vendor governance, security governance, risk management, and regulatory compliance activities throughout the organization.

This program shall be read together with:

- Compliance Governance Framework
- Data Retention, Deletion, and Secure Disposal Policy
- Artificial Intelligence Governance Program
- AI Consent Framework
- Information Security Program
- Incident Response Program
- Vendor Governance Program
- Business Continuity Program
- Disaster Recovery Program
- HealScript™ Governance Requirements
- HealConnect™ Governance Requirements
- CogneraAI™ Governance Requirements

Together, these governance programs establish the foundation for responsible healthcare technology operations.

30.13 Final Commitment

Cognera Health remains committed to protecting the information entrusted to the organization through responsible governance, ethical practices, transparent operations, secure technologies, accountable leadership, and continuous improvement.

The organization shall continue to evolve its privacy, security, compliance, information governance, and artificial intelligence governance programs to address emerging technologies, evolving risks, changing regulations, and the needs of the individuals, organizations, and communities it serves.

The objective is to maintain a trusted, secure, transparent, accountable, privacy-conscious, ethically governed, and enterprise-grade healthcare technology environment capable of supporting the future of continuous care, behavioral health, mental health, wellness, and responsible artificial intelligence.

APPENDIX A

Privacy Governance RACI Matrix

Purpose

Establish accountability across all privacy governance activities.

Activity	Executive	Privacy	Compliance	Security	Legal	Product	Operations
Privacy Policy Approval	A	R	C	C	C	I	I
Privacy Rights	I	A/R	C	I	C	I	C
Privacy Incident Response	I	A	C	R	C	I	C
AI Governance	I	C	C	C	C	R	I
Vendor Governance	I	C	C	C	C	I	R

Legend:

- R = Responsible
- A = Accountable
- C = Consulted
- I = Informed

APPENDIX B

Privacy Risk Classification Framework

Privacy Risk Level	Description	Example Events	Required Escalation	Expected Response Priority
Critical Risk	Events that may result in significant legal, regulatory, operational, financial, privacy, security, clinical, or reputational impact to the organization or affected individuals.	• Major PHI Breach • OCR Investigation • Regulatory Enforcement Action • High-Risk AI Failure • Large-Scale Unauthorized Disclosure	**Executive Leadership**	Immediate notification and executive review. Incident response procedures initiated without delay.

	Immediate executive oversight is required.	• Material Compliance Violation		
High Risk	Events that may create substantial privacy, security, compliance, operational, or reputational risk and require senior governance review and oversight.	• Unauthorized Disclosure of Sensitive Information • Significant Vendor Incident • Material Security Event • Significant Policy Violation • Third-Party Data Exposure • Elevated AI Governance Concern	**Privacy, Security, and Compliance Steering Committee**	Prompt investigation, risk assessment, corrective action planning, and management oversight.
Moderate Risk	Events that present limited organizational impact but require management review, remediation, and monitoring.	• Limited Disclosure • Isolated Control Failure • Access Management Deficiency • Delayed Privacy Response Activity • Minor Vendor Compliance Issue	**Privacy Officer**	Timely investigation, remediation, documentation, and follow-up monitoring.
Low Risk	Events with minimal impact that can be addressed through routine operational processes and corrective actions.	• Documentation Errors • Minor Administrative Issues • Training Record Deficiencies • Non-Material Process Deviations • Minor Policy Exceptions	**Operational Management**	Routine corrective action, documentation, and process improvement as appropriate.

APPENDIX C

Privacy KPI Framework

KPI Category	KPI	Target	Measurement Frequency	Governance Owner
Governance	Privacy Policy Review Completion	100%	Annually	Privacy Officer
Governance	Annual Governance Review Completion	100%	Annually	Compliance Officer
Governance	Privacy Risk Assessments Completed	≥95%	Quarterly	Privacy Officer
Governance	Privacy Training Completion	100%	Quarterly / Annually	Human Resources & Compliance
Rights Management	Access Requests Completed Within Required Timeframe	≥95%	Monthly	Privacy Officer
Rights Management	Deletion Requests Completed Within Required Timeframe	≥95%	Monthly	Privacy Officer
Rights Management	Appeal Resolution Time	≤30 Days	Monthly	Privacy Officer
Rights Management	Complaint Resolution Time	≤30 Days	Monthly	Privacy Officer
Incident Management	Mean Time to Detect (MTTD) Privacy Incidents	Continuous Improvement	Monthly	Security & Privacy Teams
Incident Management	Mean Time to Contain (MTTC) Privacy Incidents	Continuous Improvement	Monthly	Security & Privacy Teams
Incident Management	Incident Documentation Completion	100%	Monthly	Privacy Officer
Incident Management	Root Cause Analysis Completion	100%	Monthly	Privacy Officer

AI Governance	AI Validation Completion	100%	Prior to Production Deployment	AI Governance Committee
AI Governance	Human Review Rate for High-Risk AI Activities	100%	Continuous	AI Governance Committee
AI Governance	AI Audit Completion	Quarterly	Quarterly	AI Governance Committee
AI Governance	AI Drift Review Completion	Quarterly	Quarterly	AI Governance Committee

Privacy KPI Performance Classification

KPI Performance Level	Threshold
Exceeds Target	≥ 105% of target or materially exceeds expectations
Meets Target	95%–104% of target
Needs Attention	80%–94% of target
Below Target	< 80% of target
Critical Performance Gap	Material compliance, regulatory, privacy, or security deficiency requiring escalation

KPI Reporting and Escalation Framework

KPI Status	Escalation Requirement	Review Authority
On Target	Routine monitoring	Privacy Officer
Needs Attention	Management review required	Privacy Officer
Below Target	Corrective action plan required	Compliance Officer
Critical Performance Gap	Immediate escalation and remediation	Executive Leadership & Governance Committee

APPENDIX D

Privacy Impact Assessment (PIA) Framework

PIA Required For:

- New Products
- New Platforms
- New Integrations
- New Vendors
- New AI Systems
- New Data Sharing Activities
- New Consumer Health Data Processing Activities

Assessment Areas:

- Privacy Risk
- Security Risk
- Regulatory Impact
- Consent Impact
- AI Impact
- Vendor Impact
- Retention Impact

APPENDIX E

Data Protection Impact Assessment (DPIA) Framework

Required For:

- High-Risk Processing
- AI Systems
- Behavioral Health Data
- Consumer Health Data
- Large-Scale Processing

Assessment Areas:

- Legal Basis
- Data Flows
- Risks
- Controls
- Residual Risk

- Approval Requirements

APPENDIX F

- AI Risk Assessment Framework
- Assessment Areas
- Privacy
- Security
- Fairness
- Explainability
- Transparency
- Accountability
- Clinical Impact
- Regulatory Impact
- Vendor Risk
- Data Quality

APPENDIX G

Vendor Risk Assessment Framework

Assessment Domains:

- Privacy
- Security
- Compliance
- AI Governance
- Incident Response
- Business Continuity
- Disaster Recovery
- Financial Stability
- Regulatory History
- Data Retention

APPENDIX H

Enterprise Information Classification Matrix

Classification	Examples	Controls
Restricted	PHI, ePHI, Consumer Health Data	Encryption, MFA, Logging

Confidential	Contracts, Audit Reports	Encryption, Access Controls
Internal	Procedures, Training	Access Controls
Public	Website Content	Publication Approval

APPENDIX I

Privacy Exception Management Framework

Required:

- Business Justification
- Risk Assessment
- Compensating Controls
- Approval
- Expiration Date
- Review Schedule
- Closure Documentation

APPENDIX J

Privacy Program Maturity Model

- Level 1 – Initial
  - Reactive.
- Level 2 – Developing
  - Basic governance.
- Level 3 – Defined
  - Formal governance.
- Level 4 – Managed
  - Metrics-driven.
- Level 5 – Optimized

Continuous improvement and predictive governance.

Goal: Cognera Health Target State = Level 4–5

APPENDIX K

Privacy Risk Scoring Methodology

Purpose

Establish a consistent methodology for evaluating privacy risks.

Impact Scoring

1 – Negligible
Minimal operational impact.

2 – Minor
Limited operational impact.

3 – Moderate
Material privacy concern.

4 – Significant
Major privacy exposure.

5 – Critical
Severe regulatory or customer impact.

Likelihood Scoring

- **1 – Rare**
- **2 – Unlikely**
- **3 – Possible**
- **4 – Likely**
- **5 – Almost Certain**

Risk Formula
Risk Score = Impact × Likelihood

Risk Categories

Score	Rating
1–5	Low
6–10	Moderate
11–15	High
16–25	Critical

APPENDIX L

- AI Risk Scoring Framework
- AI Risk Domains
- Privacy Risk

- Security Risk
- Clinical Risk
- Bias Risk
- Explainability Risk
- Regulatory Risk
- Vendor Risk
- Operational Risk

AI Approval Requirements

Risk	Approval
Low	AI Owner
Moderate	Privacy + Compliance
High	Steering Committee
Critical	Executive Leadership

APPENDIX M

Information Asset Inventory Standard

Required Fields:

- Asset Name
- Owner
- Steward
- Classification
- Retention Schedule
- System Location
- Regulatory Scope
- Vendor Dependencies
- AI Usage
- Data Residency
- Last Review Date

APPENDIX N

Enterprise Data Flow Mapping Standard

Each major process shall document:

- Source

- Collection Method
- Processing Activity
- Storage Location
- Internal Sharing
- External Sharing
- Retention
- Disposal
- AI Processing
- Cross-Border Transfers

APPENDIX O

Privacy by Design Review Checklist

Required Review Areas:

- Collection
- Consent
- Retention
- Security
- AI Usage
- Data Sharing
- Consumer Rights
- Vendor Usage
- Cross-Border Processing
- Regulatory Impact

APPENDIX P

Secure Development Privacy Requirements

Applies To:

- HealScript™
- HealConnect™
- CogneraAI™
- APIs

Required:

- Threat Modeling

- Privacy Reviews
- Security Reviews
- Code Reviews
- Vulnerability Reviews
- AI Reviews

APPENDIX Q

AI Model Approval Workflow

- Step 1
  - Business Justification
- Step 2
  - Privacy Review
- Step 3
  - Security Review
- Step 4
  - AI Risk Assessment
- Step 5
  - Validation Testing
- Step 6
  - Governance Approval
- Step 7
  - Production Deployment
- Step 8
  - Continuous Monitoring

APPENDIX R

Privacy Control Library

Administrative Controls

Examples:

- Policies
- Procedures
- Training
- Risk Assessments

Technical Controls

Examples:

- Encryption
- MFA
- RBAC
- Logging

Operational Controls

Examples:

- Monitoring
- Auditing
- Reviews
- Incident Response

APPENDIX S

Privacy Audit Evidence Requirements

Examples:

- Policies
- Procedures
- Training Records
- Risk Assessments
- Vendor Reviews
- Rights Requests
- Incident Records
- Audit Logs
- AI Validation Records
- Consent Records

APPENDIX T

Regulatory Response Playbook

OCR Inquiry

Required:

- Legal Review
- Privacy Review
- Evidence Collection
- Response Coordination

State Privacy Inquiry

Required:

- Compliance Review
- Legal Review
- Documentation Review

APPENDIX U

Privacy Metrics Dictionary

Each KPI shall define:

- Purpose
- Formula
- Data Source
- Review Frequency
- Owner
- Target
- Escalation Threshold

APPENDIX V

Enterprise Governance Calendar

Monthly:

- Rights Review
- Complaint Review
- Incident Review

Quarterly:

- Risk Assessments
- Vendor Reviews

- AI Reviews
- Governance Reviews

Annually:

- Program Review
- Policy Review
- Training Refresh
- Maturity Assessment

APPENDIX W

Privacy Training Curriculum

Required Modules:

- HIPAA
- Privacy Governance
- Security Awareness
- AI Governance
- Consumer Health Data
- Vendor Governance
- Incident Reporting
- Records Management

APPENDIX X

- Data Governance Committee Charter
- Responsibilities:
- Governance Oversight
- Policy Approval
- Risk Oversight
- AI Governance
- Vendor Governance
- Strategic Direction

APPENDIX Y

Privacy Program Maturity Assessment

Domains:

- Governance
- Privacy
- Security
- AI
- Vendors
- Rights
- Retention
- Incident Response
- Compliance
- Metrics

Scoring: 1–5

Tracked annually.

APPENDIX Z

Privacy Program Roadmap

- Year 1
  - Foundational Governance
- Year 2
  - Operational Excellence
- Year 3
  - Automation & Intelligence
- Year 4
  - Predictive Governance
- Year 5
  - Optimized Enterprise Governance

APPENDIX AA

Enterprise Control Mapping Matrix

Purpose

This Control Mapping Matrix identifies how the Cognera Health™ Privacy & Data Protection Program aligns with applicable healthcare, privacy, cybersecurity, artificial intelligence, records management, and governance requirements.

The matrix is intended to support:

- Regulatory Readiness
- Audit Readiness
- Customer Due Diligence
- Vendor Assessments
- Governance Reviews
- Compliance Monitoring
- Control Validation

Section	HIPAA Privacy Rule	HIPAA Security Rule	HIPAA Breach Rule	HITECH	GDPR	UK GDPR	CCPA / CPRA	HITRUST CSF	ISO 27001 Annex A	ISO 27701	NIST CSF	NIST 800-53	NIST AI RMF
1 Purpose	✓	✓	✓	✓	Art.5	✓	✓	Governance	A.5	P.5	Govern	PM	Govern
2 Scope	✓	✓	✓	✓	Art.5	✓	✓	Governance	A.5	P.5	Govern	PM	Govern
3 Regulatory Alignment	✓	✓	✓	✓	Art.5-21	✓	✓	All Domains	A.5	P.5	Govern	PM	Govern
4 Privacy Governance	✓	✓	✓	✓	Art.5	✓	✓	Governance	A.5	P.5	Govern	PM	Govern
5 Privacy Principles	✓	✓	✓	✓	Art.5	✓	✓	Governance	A.5	P.5	Govern	PM	Govern
6 Roles & Responsibilities	✓	✓	✓	✓	Art.24	✓	✓	Governance	A.5.2	P.5	Govern	PM	Govern
7 Information Governance	✓	✓	✓	✓	Art.5	✓	✓	Information Protection	A.5, A.8	P.7	Identify	MP	Govern
8 Collection Governance	✓			✓	Art.5,6,13	✓	✓	Privacy Practices	A.5	P.7	Identify	AR	Govern

Section	HIPAA Privacy Rule	HIPAA Security Rule	HIPAA Breach Rule	HITECH	GDPR	UK GDPR	CCPA / CPRA	HITRUST CSF	ISO 27001 Annex A	ISO 27701	NIST CSF	NIST 800-53	NIST AI RMF
9 Processing Governance	✓	✓		✓	Art.5,6,9	✓	✓	Privacy Program	A.5, A.8	P.7	Protect	AC	Govern
10 HealScript™ Governance	✓	✓	✓	✓	Art.5	✓	✓	Healthcare Controls	A.8	P.7	Protect	AC, AU	Govern
11 HealConnect™ Governance	✓	✓		✓	Art.5	✓	✓	Consumer Health Controls	A.8	P.7	Protect	AC	Govern
12 CogneraAI™ Governance	✓	✓		✓	Art.22	✓	✓	Emerging Controls	A.5, A.8	P.8	Govern	RA	Govern, Map, Measure
13 Voice Governance	✓	✓	✓	✓	Art.9	✓	✓	Sensitive Data	A.8, A.10	P.7	Protect	AC, SC	Govern
14 Consent Governance	✓			✓	Art.6,7	✓	✓	Privacy Rights	A.5	P.7	Govern	AR	Govern
15 Sharing Governance	✓	✓	✓	✓	Art.13,14	✓	✓	Third Party Controls	A.5, A.15	P.8	Protect	AC, CA	Govern
16 HIPAA Governance	✓	✓	✓	✓				Healthcare Controls	A.5	P.6	Govern	AC, AU	Govern
17 Privacy Rights	✓			✓	Art.15-21	✓	✓	Privacy Rights	A.5	P.7	Govern	AR	Govern
18 Consumer Privacy Rights					Art.15-21	✓	✓	Privacy Rights	A.5	P.7	Govern	AR	Govern
19 Responsible AI Program		✓			Art.22	✓	✓	Emerging Controls	A.5, A.8	P.8	Govern	RA, CA	Govern, Map, Measure, Manage
20 International Transfers		✓			Art.44-49	✓	✓	Third Party Controls	A.5	P.8	Govern	CA	Govern
21 Retention & Disposal	✓	✓		✓	Art.5	✓	✓	Records Management	A.5, A.8	P.7	Protect	MP	Govern
22 Security Safeguards		✓	✓	✓	Art.32	✓	✓	Information Protection	A.5-A.8	P.6	Protect, Detect	AC, AU, SC, SI	Govern
23 Incident Response	✓	✓	✓	✓	Art.33,34	✓	✓	Incident Mgmt	A.5	P.6	Respond	IR	Govern
24 Vendor Governance	✓	✓	✓	✓	Art.28	✓	✓	Third Party Assurance	A.15	P.8	Govern	SA, SR	Govern
25 Complaints Program	✓			✓	Art.77	✓	✓	Governance	A.5	P.5	Govern	PM	Govern
26 Privacy Office	✓	✓	✓	✓	Art.37	✓	✓	Governance	A.5	P.5	Govern	PM	Govern
27 Glossary	Supportive	Supportive	Supportive	Supportive	Supportive	Supportive	Supportive	Governance	A.5	P.5	Govern	PM	Govern

Section	HIPAA Privacy Rule	HIPAA Security Rule	HIPAA Breach Rule	HITECH	GDPR	UK GDPR	CCPA / CPRA	HITRUST CSF	ISO 27001 Annex A	ISO 27701	NIST CSF	NIST 800-53	NIST AI RMF
28 References	Supportive	Supportive	Supportive	Supportive	Supportive	Supportive	Supportive	Governance	A.5	P.5	Govern	PM	Govern
29 Document Governance	✓	✓	✓	✓	Art.24	✓	✓	Governance	A.5	P.5	Govern	PM	Govern
30 Conclusion	Supportive	Supportive	Supportive	Supportive	Supportive	Supportive	Supportive	Governance	A.5	P.5	Govern	PM	Govern

Key Framework Mapping Legend

Framework / Standard	Primary Areas	Example Controls, Requirements, or Functions
HIPAA Privacy Rule	Privacy, Use & Disclosure of PHI	• Uses and Disclosures • Minimum Necessary Standard • Individual Privacy Rights • Authorizations and Consents • Business Associate Requirements
HIPAA Security Rule	Protection of ePHI	• Administrative Safeguards • Technical Safeguards • Physical Safeguards • Risk Analysis and Risk Management • Access Controls and Authentication
GDPR	Personal Data Protection and Privacy Rights	• Article 5 – Data Protection Principles • Article 6 – Lawful Basis for Processing • Article 9 – Special Categories of Personal Data • Article 13 – Transparency Requirements • Articles 15–21 – Data Subject Rights • Articles 44–49 – International Data Transfers
HITRUST CSF	Integrated Security, Privacy, and Risk Management Controls	• Governance • Information Protection Program • Access Control Management • Risk Management • Third-Party Assurance • Incident Management
ISO/IEC 27001 Annex A	Information Security Controls	• A.5 Organizational Controls • A.6 People Controls • A.7 Physical Controls • A.8 Technological Controls

Framework / Standard	Primary Areas	Example Controls, Requirements, or Functions
ISO/IEC 27701	Privacy Information Management System (PIMS)	• PII Governance • Privacy Risk Management • Data Subject Rights Management • Third-Party Privacy Governance
NIST Cybersecurity Framework (CSF)	Cybersecurity Risk Management Functions	• Govern • Identify • Protect • Detect • Respond • Recover
NIST SP 800-53	Security and Privacy Control Families	• AC – Access Control • AU – Audit & Accountability • CA – Assessment & Authorization • IR – Incident Response • MP – Media Protection • PM – Program Management • RA – Risk Assessment • SA – System & Services Acquisition • SC – System & Communications Protection • SI – System & Information Integrity • SR – Supply Chain Risk Management
NIST AI RMF	Artificial Intelligence Risk Management	• Govern • Map • Measure • Manage

Framework Purpose Summary

Framework	Primary Focus
HIPAA Privacy Rule	Protection and appropriate use/disclosure of PHI
HIPAA Security Rule	Protection of electronic PHI (ePHI)
GDPR	Protection of personal data and privacy rights

Framework	Primary Focus
HITRUST CSF	Integrated security, privacy, and compliance assurance
ISO 27001	Information Security Management System (ISMS)
ISO 27701	Privacy Information Management System (PIMS)
NIST CSF	Enterprise cybersecurity governance and risk management
NIST SP 800-53	Detailed security and privacy control catalog
NIST AI RMF	Responsible, trustworthy, and governed AI systems

Crosswalk Usage Legend

Mapping Reference	Meaning
HIPAA-P	HIPAA Privacy Rule Requirement
HIPAA-S	HIPAA Security Rule Requirement
GDPR	GDPR Article or Requirement
HITRUST	HITRUST CSF Control Domain
ISO27001	ISO/IEC 27001 Annex A Control
ISO27701	ISO/IEC 27701 Privacy Control
NIST-CSF	NIST Cybersecurity Framework Function
NIST-800-53	NIST SP 800-53 Control Family
NIST-AI-RMF	NIST AI Risk Management Framework Function

APPENDIX AB

Section-to-Control Mapping Matrix

Purpose

This appendix maps Sections 1–30 of the Cognera Health™ Privacy & Data Protection Program to specific regulatory citations, privacy requirements, security frameworks, and control families.

This matrix is intended to support:

- HIPAA readiness
- GDPR / UK GDPR readiness
- CCPA / CPRA readiness
- HITRUST readiness
- ISO 27001 readiness

- NIST 800-53 control alignment
- Customer security reviews
- Enterprise procurement reviews
- Audit preparation
- Governance validation

Important Notice:
This matrix indicates alignment, support, and control intent. It does not represent certification, legal determination, audit opinion, or regulatory attestation.

AB.1 Section-to-Control Mapping Matrix

Section	HIPAA Citation	GDPR / UK GDPR	CCPA / CPRA	HITRUST CSF Domain / Objective	ISO 27001 Annex A	NIST 800-53 Rev. 5
1. Purpose	45 CFR §164.308(a)(1)	Art. 5, 24	Notice / Accountability	Governance, Risk Management	A.5.1, A.5.2	PM-1, PM-9, PL-2
2. Scope	45 CFR §164.308(a)(1), §164.316	Art. 5, 24, 30	Notice, Categories of Data	Governance, Asset Management	A.5.9, A.5.12	PM-5, PL-2, CM-8
3. Regulatory Alignment	45 CFR §164.308(a)(1), §164.316	Art. 5, 6, 9, 12–23, 24, 32, 44–49	Consumer Rights, Sensitive PI	Compliance, Governance	A.5.31, A.5.36	PM-1, PM-9, CA-2
4. Privacy Governance Program	45 CFR §164.308(a)(1), §164.530	Art. 5, 24, 25	Accountability	Governance, Risk Management	A.5.1, A.5.4, A.5.36	PM-1, PM-9, RA-3
5. Privacy Principles	45 CFR §164.502(b), §164.514	Art. 5, 25	Data Minimization, Notice	Privacy Practices, Governance	A.5.34, A.5.35	PT-1, PT-2, AR-4
6. Roles & Responsibilities	45 CFR §164.308(a)(2), §164.530(a)	Art. 24, 37–39	Accountability	Organization of Information Security	A.5.2, A.5.4, A.6.3	PM-2, PM-13, AT-2
7. Information Governance	45 CFR §164.308(a)(1), §164.312(a), §164.316	Art. 5, 30	Data Categories	Asset Management, Information Protection	A.5.9, A.5.12, A.5.13	CM-8, AC-3, MP-2
8. Collection Governance	45 CFR §164.506, §164.508, §164.514	Art. 5, 6, 9, 13	Notice at Collection	Privacy Practices	A.5.34, A.5.35	PT-2, AR-2, AR-4
9. Processing Governance	45 CFR §164.502, §164.506, §164.514	Art. 5, 6, 9, 30	Use / Processing Disclosure	Information Protection, Privacy	A.5.34, A.8.2	PT-3, AC-3, AU-2
10. HealScript™ Governance	45 CFR §164.306, §164.308, §164.312	Art. 5, 9, 25, 32	Sensitive PI	Application Security, Access Control	A.5.15, A.8.2, A.8.9	AC-2, AC-3, AU-2, SC-13
11. HealConnect™ Governance	45 CFR §164.306, §164.308, §164.312	Art. 5, 9, 25, 32	Consumer Health Data, Sensitive PI	Application Security, Privacy	A.5.15, A.8.2, A.8.11	AC-3, AU-2, PT-2, SC-13
12. CogneraAI™ Governance	45 CFR §164.308(a)(1), §164.312	Art. 5, 22, 25, 32	Automated Decisioning / Profiling	Risk Management, Emerging Tech	A.5.8, A.8.25, A.8.28	RA-3, RA-5, CA-7, SI-4
13. Voice Governance	45 CFR §164.306, §164.312, §164.514	Art. 5, 9, 32	Sensitive PI / Biometric Data	Sensitive Data Protection	A.5.10, A.5.12, A.8.24	AC-3, SC-13, MP-6, PT-5

Section	HIPAA Citation	GDPR / UK GDPR	CCPA / CPRA	HITRUST CSF Domain / Objective	ISO 27001 Annex A	NIST 800-53 Rev. 5
14. Consent Governance	45 CFR §164.508, §164.506	Art. 6, 7, 9, 13	Consent / Opt-Out	Privacy Rights, Consent	A.5.34, A.5.35	PT-4, AR-2, AR-8
15. Information Sharing	45 CFR §164.502, §164.504, §164.506, §164.508	Art. 13, 14, 28, 30	Disclosure / Sharing	Third Party Assurance	A.5.19, A.5.20, A.5.21	AC-4, CA-3, SA-9
16. HIPAA Governance	45 CFR §164.502–§164.530	N/A	N/A	Healthcare Privacy Controls	A.5.34, A.5.36	PT-1, PT-2, AC-3, AU-2
17. Privacy Rights	45 CFR §164.524, §164.526, §164.528	Art. 12, 15–21	Access, Delete, Correct	Privacy Rights Management	A.5.34, A.5.35	PT-2, PT-3, AR-6, AR-8
18. Consumer Privacy Rights	N/A	Art. 12, 15–21	CCPA/CPRA Rights	Privacy Rights Management	A.5.34, A.5.35	PT-2, PT-3, AR-8
19. Responsible AI Program	45 CFR §164.308(a)(1), §164.312	Art. 5, 22, 25, 32	Automated Processing	Risk Management, Model Governance	A.5.8, A.8.25, A.8.28	RA-3, RA-7, CA-7, SI-4
20. Cross-Border Transfers	45 CFR §164.308(b)	Art. 44–49	Service Provider / Transfer Controls	Third Party Assurance	A.5.19, A.5.20, A.5.23	SA-9, SR-3, CA-3
21. Retention & Disposal	45 CFR §164.316(b), §164.310(d)(2)	Art. 5, 17, 30	Deletion / Retention	Records Management	A.5.33, A.8.10, A.8.11	MP-6, SI-12, AU-11
22. Security Safeguards	45 CFR §164.306, §164.308, §164.310, §164.312	Art. 32	Reasonable Security	Information Protection	A.5–A.8	AC, AU, IA, SC, SI, IR
23. Incident Response	45 CFR §164.308(a)(6), §164.400–414	Art. 33, 34	Breach Notification	Incident Management	A.5.24, A.5.25, A.5.26	IR-4, IR-6, IR-8
24. Vendor Governance	45 CFR §164.308(b), §164.314	Art. 28, 32	Service Provider / Contractor	Third Party Assurance	A.5.19–A.5.23	SA-9, SR-3, SR-5
25. Complaints Program	45 CFR §164.530(d), §164.530(g)	Art. 77	Consumer Requests / Complaints	Privacy Governance	A.5.34, A.5.36	PT-1, PM-9
26. Privacy Office	45 CFR §164.530(a)	Art. 37–39	Accountability	Governance	A.5.2, A.5.4	PM-2, PM-13
27. Glossary	45 CFR §164.316	Art. 12, 24	Notice Clarity	Governance Documentation	A.5.1, A.5.37	PL-2, PM-1

Section	HIPAA Citation	GDPR / UK GDPR	CCPA / CPRA	HITRUST CSF Domain / Objective	ISO 27001 Annex A	NIST 800-53 Rev. 5
28. References	45 CFR §164.316	Art. 24	Accountability	Compliance Governance	A.5.31, A.5.36	CA-2, PM-9
29. Document Governance	45 CFR §164.316	Art. 24, 30	Accountability	Policy Governance	A.5.1, A.5.37	PL-2, PM-1, CM-3
30. Conclusion	45 CFR §164.308(a)(1)	Art. 5, 24	Accountability	Governance	A.5.1	PM-1, PM-9

Appendix AB.2 – Frequently Used HIPAA Citations

Regulatory Area	Citation	Description
HIPAA Privacy Rule	45 CFR §164.502	Uses and disclosures of PHI
HIPAA Privacy Rule	45 CFR §164.504	Organizational requirements and Business Associate provisions
HIPAA Privacy Rule	45 CFR §164.506	Uses and disclosures for Treatment, Payment, and Healthcare Operations (TPO)
HIPAA Privacy Rule	45 CFR §164.508	Uses and disclosures requiring authorization
HIPAA Privacy Rule	45 CFR §164.514	De-identification and minimum necessary requirements
HIPAA Privacy Rule	45 CFR §164.520	Notice of Privacy Practices
HIPAA Privacy Rule	45 CFR §164.524	Individual right of access
HIPAA Privacy Rule	45 CFR §164.526	Individual right to amendment
HIPAA Privacy Rule	45 CFR §164.528	Accounting of disclosures
HIPAA Privacy Rule	45 CFR §164.530	Administrative requirements
HIPAA Security Rule	45 CFR §164.306	General security standards
HIPAA Security Rule	45 CFR §164.308(a)(1)	Security management process
HIPAA Security Rule	45 CFR §164.308(a)(2)	Assigned security responsibility
HIPAA Security Rule	45 CFR §164.308(a)(5)	Security awareness and training
HIPAA Security Rule	45 CFR §164.308(a)(6)	Security incident procedures
HIPAA Security Rule	45 CFR §164.308(a)(7)	Contingency planning
HIPAA Security Rule	45 CFR §164.308(a)(8)	Evaluation
HIPAA Security Rule	45 CFR §164.308(b)	Business Associate contracts and arrangements
HIPAA Security Rule	45 CFR §164.310	Physical safeguards
HIPAA Security Rule	45 CFR §164.312(a)	Access control
HIPAA Security Rule	45 CFR §164.312(b)	Audit controls
HIPAA Security Rule	45 CFR §164.312(c)	Integrity
HIPAA Security Rule	45 CFR §164.312(d)	Person or entity authentication
HIPAA Security Rule	45 CFR §164.312(e)	Transmission security
HIPAA Security Rule	45 CFR §164.314	Organizational requirements
HIPAA Security Rule	45 CFR §164.316	Policies, procedures, and documentation requirements
HIPAA Breach Notification Rule	45 CFR §§164.400–414	Breach notification requirements

Appendix AB.3 – Frequently Used GDPR / UK GDPR Articles

GDPR Article	Subject Matter
Article 5	Processing principles
Article 6	Lawful basis for processing
Article 7	Consent
Article 9	Special category data
Article 12	Transparent communication
Article 13	Information provided at collection
Article 14	Information where data is not collected directly from the individual
Article 15	Right of access
Article 16	Right to rectification
Article 17	Right to erasure ("Right to be Forgotten")
Article 18	Right to restriction of processing
Article 20	Right to data portability
Article 21	Right to object
Article 22	Automated decision-making and profiling
Article 24	Controller responsibility
Article 25	Data protection by design and by default
Article 28	Processor obligations
Article 30	Records of processing activities
Article 32	Security of processing
Article 33	Personal data breach notification to supervisory authority
Article 34	Communication of breach to affected individuals
Articles 37–39	Data Protection Officer (DPO) responsibilities
Articles 44–49	International data transfers

Appendix AB.4 – ISO/IEC 27001:2022 Annex A Control References

Control Domain	Control Reference	Description
Organizational Controls	A.5.1	Policies for information security
Organizational Controls	A.5.2	Information security roles and responsibilities
Organizational Controls	A.5.4	Management responsibilities
Organizational Controls	A.5.8	Information security in project management
Organizational Controls	A.5.9	Inventory of information and associated assets
Organizational Controls	A.5.10	Acceptable use of information and assets
Organizational Controls	A.5.12	Classification of information
Organizational Controls	A.5.13	Labelling of information
Organizational Controls	A.5.15	Access control
Organizational Controls	A.5.19	Information security in supplier relationships
Organizational Controls	A.5.20	Addressing information security within supplier agreements
Organizational Controls	A.5.21	Managing information security in the ICT supply chain

Control Domain	Control Reference	Description
Organizational Controls	A.5.23	Information security for cloud services
Organizational Controls	A.5.24	Incident management planning and preparation
Organizational Controls	A.5.25	Assessment and decision on information security events
Organizational Controls	A.5.26	Response to information security incidents
Organizational Controls	A.5.31	Legal, statutory, regulatory, and contractual requirements
Organizational Controls	A.5.33	Protection of records
Organizational Controls	A.5.34	Privacy and protection of PII
Organizational Controls	A.5.35	Independent review of information security
Organizational Controls	A.5.36	Compliance with policies, rules, and standards
Organizational Controls	A.5.37	Documented operating procedures
People Controls	A.6.3	Information security awareness, education, and training
Technological Controls	A.8.2	Privileged access rights
Technological Controls	A.8.9	Configuration management
Technological Controls	A.8.10	Information deletion
Technological Controls	A.8.11	Data masking
Technological Controls	A.8.12	Data leakage prevention
Technological Controls	A.8.15	Logging
Technological Controls	A.8.16	Monitoring activities
Technological Controls	A.8.24	Use of cryptography
Technological Controls	A.8.25	Secure development lifecycle
Technological Controls	A.8.28	Secure coding

Appendix AB.5 – NIST SP 800-53 Rev. 5 Control Families

Control Family	Control Family Name	Primary Focus
AC	Access Control	Identity, authorization, and access management
AT	Awareness and Training	Workforce security education and training
AU	Audit and Accountability	Logging, monitoring, and accountability
CA	Assessment, Authorization, and Monitoring	Security assessments and continuous monitoring
CM	Configuration Management	Secure configuration and change control

Control Family	Control Family Name	Primary Focus
CP	Contingency Planning	Business continuity and disaster recovery
IA	Identification and Authentication	User and system authentication
IR	Incident Response	Incident detection, response, and recovery
MP	Media Protection	Protection of physical and electronic media
PE	Physical and Environmental Protection	Physical security safeguards
PL	Planning	Security and privacy planning
PM	Program Management	Enterprise governance and management
PT	Personally Identifiable Information Processing and Transparency	Privacy governance and PII protection
RA	Risk Assessment	Risk identification and evaluation
SA	System and Services Acquisition	Secure development and procurement
SC	System and Communications Protection	Network and communications security
SI	System and Information Integrity	Monitoring, vulnerability management, and integrity
SR	Supply Chain Risk Management	Third-party and supply chain security management

AB.6 HITRUST Mapping Note

HITRUST CSF control IDs vary depending on:

- HITRUST CSF version
- Assessment type
- Organizational risk factors
- Regulatory factors
- System scope
- Industry applicability
- MyCSF configuration

Accordingly, this matrix maps Cognera Health program sections to HITRUST control domains and objectives rather than asserting exact HITRUST control IDs.

Exact HITRUST control references should be validated against the applicable HITRUST MyCSF assessment object before use in a formal assessment.

Common HITRUST-aligned domains include:

- Information Protection Program
- Endpoint Protection
- Portable Media Security
- Mobile Device Security
- Wireless Security
- Configuration Management
- Vulnerability Management
- Network Protection
- Transmission Protection
- Password Management
- Access Control
- Audit Logging and Monitoring
- Education, Training, and Awareness
- Third Party Assurance
- Incident Management
- Business Continuity and Disaster Recovery
- Risk Management
- Privacy Practices
- Compliance Management
- Information Security Governance

AB.7 Usage Guidance

This matrix shall be used to support:

- Internal compliance reviews.
- Privacy governance reviews.
- Customer security questionnaires.
- Procurement reviews.
- Vendor due diligence.
- Audit planning.
- Risk assessments.
- Control testing.
- HITRUST readiness.

- ISO 27001 readiness.
- HIPAA readiness.

This matrix shall be reviewed at least annually and updated following:

- Regulatory changes.
- Framework changes.
- Major product changes.
- Major AI system changes.
- Significant incidents.
- Customer requirements.
- Audit findings.

Executive Approval and Attestation

The Cognera Health™ Privacy & Data Protection Program Version 3.0 represents the organization's formal privacy governance framework and establishes enterprise requirements governing privacy, data protection, information governance, artificial intelligence governance, records management, vendor governance, cybersecurity governance, and regulatory compliance activities.

Executive Leadership affirms its commitment to:

- Privacy Protection
- Information Stewardship
- Security Governance
- Responsible Artificial Intelligence
- Regulatory Compliance
- Risk Management
- Continuous Improvement

This program shall be reviewed at least annually and updated as necessary to address regulatory changes, technological developments, organizational changes, emerging risks, customer requirements, and governance improvements.

Approval Authority

Privacy Officer

Signature: _____

Date: _____

Compliance Officer

Signature: _____

Date: _____

Chief Information Security Officer

Signature: _____

Date: _____

Legal Counsel

Signature: _____

Date: _____

Data Governance Steering Committee Chair

Signature: _____

Date: _____

Executive Leadership Representative

Signature: _____

Date: _____

Effective Date

Next Review Date

Document Classification

Confidential – Internal Governance Document

Document Status

Approved