CONFIDENTIAL | PROPRIETARY | RESTRICTED

COGNERA HEALTH™ PLATFORM GOVERNANCE, TERMS, SECURITY, PRIVACY, ACCESSIBILITY & RESPONSIBLE AI FRAMEWORK

NOTICE OF CONFIDENTIALITY

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

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

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

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

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

Any unauthorized use may result in:

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

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

Table of Contents

PART I – INTRODUCTION

1. PURPOSE

1.1 Purpose of Framework

The Cognera Health™ Platform Governance, Terms, Security, Privacy, Accessibility & Responsible AI Framework ("Framework") establishes the governance, operational, legal, privacy, security, accessibility, compliance, and responsible artificial intelligence principles governing the design, development, deployment, operation, maintenance, support, and use of Cognera Health products and services.

This Framework is intended to provide transparency regarding how Cognera Health manages information, technology, artificial intelligence, privacy, cybersecurity, accessibility, compliance obligations, operational controls, and organizational responsibilities.

This Framework serves as the primary public governance document for Cognera Health and is intended to complement, but not replace, product-specific agreements, privacy notices, customer agreements, Business Associate Agreements, Data Processing Addenda, Statements of Work, Service Level Agreements, consent forms, and applicable legal requirements.

The objective of this Framework is to communicate Cognera Health's commitment to privacy, security, transparency, accountability, responsible innovation, accessibility, and continuous improvement while supporting healthcare organizations, clinicians, care teams, individuals, and enterprise customers.

1.2 Governance Objectives

Cognera Health maintains governance programs designed to support trustworthy, secure, compliant, responsible, and resilient operation of healthcare technology services.

Governance objectives include:

- Protection of personal information
- Protection of Protected Health Information (PHI)
- Protection of electronic Protected Health Information (ePHI)
- Protection of consumer health data
- Protection of confidential information
- Responsible use of Artificial Intelligence

- Security and resilience of services
- Compliance with applicable laws and regulations
- Continuous monitoring and improvement
- Transparency and accountability
- Accessibility and inclusive design
- Responsible data stewardship

Governance activities are intended to support safe and effective use of technology while maintaining appropriate human oversight and organizational accountability.

1.3 Trust and Transparency Commitments

Cognera Health recognizes that trust is fundamental to healthcare, behavioral health, wellness, and care coordination technologies.

Accordingly, Cognera Health seeks to provide clear information regarding:

- Information processing practices
- Security safeguards
- Privacy protections
- AI governance practices
- Accessibility commitments
- Compliance programs
- Risk management activities
- Incident response procedures
- User rights
- Data lifecycle management

Cognera Health believes that transparency promotes accountability and enables customers, users, regulators, partners, and stakeholders to make informed decisions regarding the use of technology and services.

1.4 Responsible Technology Principles

Cognera Health technology programs are guided by the following principles:

Safety
Technology should support safe healthcare and operational practices.

Privacy

Information should be handled responsibly and in accordance with applicable legal and contractual requirements.

Security
Systems should be designed and operated using security safeguards appropriate to the risks presented.

Human Oversight
Technology should augment human expertise rather than replace professional judgment.

Accessibility
Technology should be designed to support equitable access and usability.

Transparency
Users should understand when technology, automation, or AI functionality is being used.

Accountability
Organizations and individuals remain responsible for decisions made using technology-assisted information.

Continuous Improvement
Governance programs should evolve in response to technological, regulatory, operational, and security developments.

1.5 Risk Management Philosophy

Cognera Health maintains a risk-based approach to governance, privacy, security, compliance, accessibility, artificial intelligence, operational resilience, and technology management.

Risk management activities shall include:

- Risk identification
- Risk assessment
- Risk treatment
- Risk acceptance
- Risk monitoring
- Risk reporting
- Risk remediation

Risk decisions are evaluated using the context of:

- Legal obligations

- Regulatory obligations
- Customer requirements
- Industry standards
- Operational considerations
- Privacy considerations
- Security considerations
- Clinical considerations
- Organizational objectives

No governance, privacy, security, compliance, accessibility, or technology program can eliminate all risks. Accordingly, Cognera Health seeks to identify, evaluate, mitigate, monitor, and manage risks using reasonable and appropriate measures.

2. SCOPE

2.1 Services Covered

This Framework applies to Cognera Health services including:

- HealScript™
- HealConnect™
- CogneraAI™
- APIs
- Integrations
- Analytics services
- Reporting services
- Documentation services
- Clinical intelligence services
- Operational intelligence services
- Enterprise intelligence services
- Data processing services
- Future successor products

The Framework applies regardless of whether services are accessed directly or through authorized integrations, approved third-party technologies, mobile applications, customer deployments, or enterprise implementations.

2.2 Technologies Covered

This Framework applies to technologies including:

- Software applications
- Mobile applications
- Cloud infrastructure
- Artificial intelligence systems
- Machine learning systems
- Natural Language Processing technologies
- Natural Language Understanding technologies
- Voice-to-text technologies
- Automation technologies
- Reporting technologies
- Analytics technologies
- Security technologies
- Administrative systems
- Operational systems
- Customer support systems

2.3 Personnel Covered

This Framework applies to:

- Employees
- Contractors
- Consultants
- Temporary personnel
- Interns
- Service providers
- Third-party vendors
- Subcontractors
- Authorized representatives

where such individuals perform activities involving Cognera Health systems, services, infrastructure, information, or operations.

3. INTENDED AUDIENCE

This Framework is intended for:

Individuals

Individuals using Cognera Health services for engagement, wellness, communication, education, monitoring, support, or care coordination purposes.

Healthcare Providers

Licensed professionals utilizing Cognera Health technologies in connection with care delivery, documentation, coordination, analytics, operational activities, or related functions.

Healthcare Organizations

Healthcare providers, clinics, health systems, group practices, integrated care organizations, wellness organizations, and related entities.

Enterprise Customers

Organizations evaluating, implementing, purchasing, licensing, deploying, or utilizing Cognera Health products and services.

Regulators

Government agencies, supervisory authorities, auditors, accreditation bodies, and other regulatory stakeholders.

Security Researchers

Individuals engaged in lawful and responsible security testing activities consistent with applicable law and Cognera Health vulnerability disclosure requirements.

Investors and Partners

Organizations evaluating Cognera Health governance, risk management, privacy, security, compliance, AI governance, accessibility, and operational maturity.

4. RELATIONSHIP TO PRIVACY POLICY

This Framework should be read together with the Cognera Health Privacy Policy.

The Privacy Policy provides detailed information regarding:

- Information collection
- Information use
- Information sharing
- Data retention
- Data deletion
- User rights
- Privacy rights
- Data subject rights
- Consumer health data rights

Where differences exist between this Framework and the Privacy Policy regarding information processing activities, the Privacy Policy shall govern those specific processing activities unless otherwise required by law or contract.

5. RELATIONSHIP TO TRUST CENTER

The Cognera Health Trust Center serves as the public-facing transparency portal for privacy, security, compliance, accessibility, governance, responsible AI, and operational resilience information.

The Trust Center shall provide:

- Governance summaries
- Compliance information
- Security information
- Privacy information
- AI governance information
- Accessibility information
- Data retention information
- Data deletion information
- Contact information

The Trust Center is informational in nature and shall be updated periodically to reflect changes in governance practices, technologies, products, legal requirements, or organizational operations.

6. RELATIONSHIP TO ENTERPRISE AGREEMENTS

This Framework is intended to provide public transparency regarding Cognera Health governance, privacy, security, accessibility, compliance, artificial intelligence governance, operational resilience, and related practices.

This Framework is not intended to replace executed contractual agreements.

Customers shall be subject to additional contractual obligations through:

- Master Services Agreements (MSA)
- Order Forms
- Statements of Work (SOW)
- Business Associate Agreements (BAA)
- Data Processing Addenda (DPA)
- Service Level Agreements (SLA)
- Security Exhibits
- Responsible AI Addenda
- Telehealth Addenda
- Professional Services Agreements
- Enterprise Licensing Agreements

Where an executed agreement conflicts with this Framework, the executed agreement shall generally govern with respect to the applicable customer relationship unless otherwise prohibited by law.

Certain services, features, integrations, deployments, or customer-specific implementations shall also be subject to supplemental terms, operational requirements, implementation documentation, technical specifications, customer instructions, privacy notices, or regulatory requirements.

Nothing in this Framework shall be interpreted to limit obligations imposed by applicable law, regulatory requirements, contractual obligations, accreditation requirements, professional standards, or customer-specific agreements.

7. DEFINITIONS

The following definitions apply throughout this Framework.

7.1 Artificial Intelligence (AI)

Artificial Intelligence ("AI") refers to computational technologies that perform functions traditionally associated with human cognitive activities, including but not limited to pattern recognition, prediction, classification, summarization, recommendation generation, workflow automation, information extraction, natural language processing, reasoning support, and decision-support functions.

AI shall include machine learning models, natural language processing systems, natural language understanding systems, large language models, predictive analytics systems, automation systems, recommendation systems, statistical models, hybrid models, and related technologies.

AI systems shall operate using structured data, unstructured data, textual information, audio information, operational information, clinical information, behavioral information, wellness information, user-generated information, or other data sources.

AI systems utilized by Cognera Health are intended to support human users and are not intended to independently replace professional judgment, clinical decision-making, emergency response activities, or human oversight responsibilities.

7.2 AI Output

AI Output refers to any content, information, recommendation, summary, classification, prediction, alert, workflow suggestion, documentation draft, generated text, generated analysis, generated insight, generated response, generated report, generated transcription, generated interpretation, or other output produced wholly or partially through AI-enabled functionality.

AI Outputs shall be generated automatically or semi-automatically.

AI Outputs shall contain inaccuracies, omissions, hallucinations, outdated information, incomplete information, unintended bias, or other limitations.

AI Outputs should be independently reviewed and validated before being relied upon for clinical, operational, financial, compliance, legal, regulatory, administrative, or business purposes.

7.3 Authorized User

Authorized User means an individual who has been granted permission to access, use, administer, support, manage, supervise, review, monitor, configure, or otherwise interact with Cognera Health services.

Authorized Users shall include:

- Licensed healthcare professionals
- Clinical supervisors
- Organizational administrators
- Operational personnel
- Support personnel
- Care coordinators
- Enterprise users
- Authorized individuals

Authorized Users are responsible for complying with applicable laws, contracts, organizational policies, security requirements, privacy requirements, and platform requirements.

7.4 Customer

Customer means an individual, organization, healthcare provider, healthcare system, employer, university, government entity, enterprise organization, clinic, wellness organization, payer, or other entity that licenses, subscribes to, purchases, accesses, implements, deploys, evaluates, or otherwise utilizes Cognera Health products or services.

The term Customer includes both prospective and existing customers where applicable.

7.5 Covered Entity

Covered Entity shall have the meaning assigned under HIPAA and generally includes:

- Healthcare providers
- Health plans
- Healthcare clearinghouses

and other entities subject to HIPAA requirements.

Where applicable, Cognera Health shall provide services to Covered Entities pursuant to contractual arrangements and Business Associate Agreements.

7.6 Business Associate

Business Associate shall have the meaning assigned under HIPAA.

Where Cognera Health creates, receives, maintains, processes, stores, transmits, or otherwise handles Protected Health Information on behalf of a Covered Entity, Cognera Health shall operate as a Business Associate pursuant to applicable Business Associate Agreements and applicable law.

Business Associate activities are subject to contractual, legal, regulatory, privacy, and security obligations.

7.7 Consumer Health Data

Consumer Health Data refers to information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to an individual's physical health, mental health, behavioral health, wellness status, healthcare services, healthcare utilization, health-related activities, health-related preferences, symptoms, conditions, diagnoses, treatments, medications, assessments, outcomes, or other health-related characteristics.

Consumer Health Data shall be regulated by state privacy laws, consumer health privacy laws, healthcare regulations, contractual obligations, or other legal requirements.

7.8 Protected Health Information (PHI)

Protected Health Information ("PHI") refers to individually identifiable health information protected under HIPAA.

PHI shall include:

- Clinical records
- Treatment records
- Assessments
- Progress notes
- Care plans

- Behavioral health information
- Wellness information
- Health-related communications
- Health-related identifiers

PHI shall exist in electronic, paper, verbal, audio, visual, or other forms.

7.9 Electronic Protected Health Information (ePHI)

Electronic Protected Health Information ("ePHI") refers to PHI that is created, received, maintained, processed, stored, transmitted, archived, or otherwise handled in electronic form.

ePHI shall exist within:

- Databases
- Cloud environments
- Applications
- APIs
- Reporting systems
- Analytics platforms
- Backup systems
- Mobile applications
- Communication systems

ePHI is subject to applicable privacy and security safeguards.

7.10 Personal Data

Personal Data refers to information relating to an identified or identifiable individual.

Personal Data shall include:

- Names
- Email addresses
- Phone numbers
- Device identifiers
- Account information
- Location information

- Online identifiers
- User-generated information
- Demographic information
- Other identifying information

Personal Data shall be regulated under GDPR, UK GDPR, CCPA, CPRA, state privacy laws, consumer health privacy laws, and other applicable privacy regulations.

7.11 Platform

Platform refers collectively to:

- Cognera Health™
- HealScript™
- HealConnect™
- CogneraAI™
- Mobile applications
- Websites
- APIs
- Integrations
- Reporting systems
- Analytics systems
- Operational intelligence systems
- Clinical intelligence systems
- Enterprise intelligence systems

and related services.

The Platform shall include current and future products, services, modules, integrations, and functionality.

7.12 Services

Services means any product, software, application, website, platform, integration, API, feature, functionality, support activity, implementation activity, reporting service, analytics service, professional service, operational service, or technology offering provided by Cognera Health.

Services shall be delivered directly or through authorized partners, service providers, integrations, or approved third-party technologies.

7.13 Telehealth

Telehealth refers to technology-enabled healthcare communication, coordination, consultation, monitoring, engagement, education, support, documentation, workflow, collaboration, or related activities conducted through electronic means.

Telehealth activities shall include:

- Video communication
- Audio communication
- Messaging
- Care coordination
- Documentation
- Monitoring
- Engagement activities

The existence of telehealth functionality does not mean Cognera Health is providing healthcare services.

Healthcare services remain the responsibility of licensed healthcare providers.

PART II – PRODUCTS COVERED

8. COGNERA HEALTH™ PLATFORM OVERVIEW

8.1 Platform Purpose

Cognera Health™ is a cloud-based healthcare technology platform designed to support continuous, connected, coordinated, and intelligence-driven care delivery across mental health, behavioral health, wellness, integrated care, care coordination, population health, and related healthcare environments.

The platform is designed to address limitations commonly associated with fragmented healthcare systems, disconnected workflows, administrative burden, limited visibility between encounters, delayed interventions, documentation inefficiencies, and siloed information systems.

Cognera Health seeks to support healthcare organizations, clinicians, care teams, administrators, operational leaders, and individuals through technology-enabled workflows, data integration, analytics, automation, engagement tools, and responsible artificial intelligence capabilities.

The platform is designed to facilitate collaboration among authorized users while maintaining privacy, security, governance, compliance, accessibility, and operational oversight requirements.

8.2 Continuous Care Philosophy

Traditional healthcare delivery often focuses on episodic interactions occurring during appointments, encounters, or scheduled engagements.

Cognera Health is designed to support a continuous care model intended to provide greater visibility between encounters, support longitudinal monitoring, improve care coordination, facilitate earlier identification of issues, enhance engagement, and provide operational intelligence across the care continuum.

The continuous care philosophy is based upon the concept that meaningful information shall exist between formal appointments and that technology shall assist authorized users in monitoring, organizing, documenting, reviewing, and acting upon available information.

The platform is not intended to replace professional care delivery but rather to support informed decision-making and improved operational efficiency.

8.3 Platform Architecture

The platform consists of multiple integrated technology components designed to operate as a unified ecosystem.

Core components shall include:

- Clinical Intelligence
- Operational Intelligence
- Enterprise Intelligence
- Analytics
- Documentation Services
- Assessment Services
- Care Coordination Services

- Communication Services
- AI Services
- Reporting Services
- Integration Services
- Security Services
- Compliance Services
- Governance Services

The architecture shall evolve over time as technology, regulatory requirements, operational needs, customer requirements, and industry practices change.

8.4 Intended Users

The platform shall be used by:

- Psychiatrists
- Psychologists
- Therapists
- Counselors
- Social Workers
- Care Coordinators
- Behavioral Health Professionals
- Wellness Professionals
- Clinical Supervisors
- Healthcare Administrators
- Operational Leaders
- Healthcare Organizations
- Integrated Care Teams
- Authorized Individuals

Use of the platform remains subject to applicable laws, regulations, licensing requirements, organizational policies, contractual requirements, and professional responsibilities.

9. HEALSCRIPT™

9.1 Overview

HealScript™ is the provider-facing clinical, operational, and organizational intelligence platform within the Cognera Health ecosystem.

HealScript is designed to assist healthcare professionals and organizations with clinical workflows, documentation, care coordination, operational visibility, outcome tracking, analytics, workflow management, communication, and AI-assisted functions.

HealScript serves as a centralized environment for authorized users to access information, coordinate activities, monitor performance, review trends, document services, and support care delivery activities.

HealScript does not replace clinical expertise, professional judgment, organizational policies, regulatory requirements, or applicable standards of care.

9.2 Clinical Intelligence

Clinical Intelligence functionality is intended to assist authorized users in organizing, reviewing, monitoring, and interpreting clinical information.

Clinical Intelligence capabilities shall include:

- Longitudinal data review
- Outcome measurement tracking
- Assessment monitoring
- Documentation analysis
- Trend identification
- Risk signal identification
- Care plan visibility
- Clinical workflow support

Clinical Intelligence functionality is designed as a decision-support capability.

Clinical Intelligence functionality does not independently diagnose, prescribe, determine treatment plans, or establish standards of care.

All clinical decisions remain the responsibility of licensed healthcare professionals.

9.3 Operational Intelligence

Operational Intelligence capabilities are intended to assist organizations in monitoring operational performance, workflow efficiency, utilization patterns, resource allocation, productivity trends, service delivery performance, and organizational effectiveness.

Operational Intelligence functions shall include:

- KPI dashboards
- Utilization analytics
- Workflow monitoring
- Operational reporting
- Caseload visibility
- Resource allocation visibility
- Performance monitoring
- Operational trend analysis

Operational Intelligence functionality is intended to support informed organizational decision-making and operational oversight.

9.4 Documentation Support

HealScript shall provide documentation support capabilities designed to reduce administrative burden and improve documentation efficiency.

Documentation support shall include:

- Progress note generation assistance
- SOAP note assistance
- DAP note assistance
- BIRP note assistance
- Session summaries
- Documentation templates
- Documentation recommendations
- Voice-to-text functionality
- Clinical transcription

Documentation support features shall use automation and artificial intelligence technologies.

All documentation generated or assisted by the platform must be reviewed and validated by authorized personnel before use.

The user remains responsible for the accuracy, completeness, appropriateness, and regulatory compliance of all documentation.

9.5 Measurement-Based Care

HealScript shall support measurement-based care activities through the collection, organization, presentation, analysis, and reporting of assessment information and outcome measures.

Supported activities shall include:

- Assessment administration
- Assessment tracking
- Outcome monitoring
- Progress monitoring
- Historical comparisons
- Longitudinal reporting
- Trend analysis
- Clinical review support

Measurement-based care functionality is intended to provide information to support clinical decision-making and quality improvement efforts.

9.6 Analytics

Analytics functionality shall provide:

- Clinical analytics
- Operational analytics
- Organizational analytics
- Utilization analytics
- Outcome analytics
- Population analytics
- Quality analytics
- Productivity analytics

Analytics outputs should be interpreted within the context of professional expertise, organizational objectives, data quality limitations, and operational realities.

Analytics outputs should not be interpreted as guarantees, predictions, or assurances regarding future outcomes.

9.7 Care Coordination

Care coordination functionality is intended to support collaboration among authorized participants in care delivery and operational activities.

Care coordination functions shall include:

- Shared visibility
- Team communication
- Care planning support
- Follow-up management
- Workflow coordination
- Referral tracking
- Escalation workflows
- Case management support

The platform facilitates information exchange but does not replace professional responsibilities related to coordination, communication, supervision, or care delivery.

9.8 Reporting

HealScript shall generate reports intended to support:

- Clinical review
- Operational review
- Organizational oversight
- Regulatory reporting
- Quality improvement
- Utilization review
- Compliance monitoring
- Management activities

Reports shall be based upon available information at the time of generation and shall be affected by data quality, timing, completeness, integration status, user activity, and other factors.

Users are responsible for reviewing reports before relying upon them.

9.9 Provider Productivity

HealScript shall provide tools intended to support provider efficiency, workflow optimization, administrative burden reduction, task management, scheduling support, and documentation assistance.

Productivity functionality is intended to support healthcare professionals in performing administrative and operational tasks more efficiently.

Productivity functionality does not replace professional accountability or regulatory obligations.

9.10 AI Assistance

HealScript shall utilize CogneraAI™ functionality to support:

- Documentation assistance
- Summarization
- Trend analysis
- Workflow automation
- Recommendation generation
- Administrative assistance
- Reporting support
- Operational intelligence

AI assistance features are subject to all requirements contained within this Framework regarding responsible AI governance, human oversight, validation requirements, transparency requirements, and AI limitations.

AI-generated outputs must be independently reviewed before use.

10. HEALCONNECT™

10.1 Overview

HealConnect™ is the individual-facing engagement and continuity platform within the Cognera Health ecosystem.

HealConnect is designed to facilitate engagement, communication, monitoring, journaling, assessments, reminders, education, continuity-of-care activities, and related support functions between formal encounters.

HealConnect is intended to support engagement and information sharing.

HealConnect does not provide medical care, psychotherapy, psychiatric treatment, crisis intervention, emergency services, diagnosis, prescribing services, or professional healthcare services.

The platform functions as a technology tool and communication environment supporting authorized healthcare workflows.

10.2 Assessments

HealConnect™ shall facilitate the administration, collection, organization, presentation, monitoring, and transmission of assessments, questionnaires, surveys, outcome measures, screening instruments, wellness evaluations, symptom tracking instruments, and other structured information collection tools.

Assessment functionality is intended to support engagement, monitoring, continuity-of-care activities, measurement-based care activities, and communication between authorized participants.

Assessment functionality shall support:

- Mental health assessments
- Behavioral health assessments
- Wellness assessments
- Outcome measurements
- Symptom monitoring
- Progress evaluations
- Risk screening instruments
- Organization-specific assessments

Assessment results are informational and should not be interpreted as diagnoses, treatment recommendations, medical advice, or professional conclusions unless independently reviewed and interpreted by qualified professionals.

Assessment functionality does not replace clinical evaluation, professional judgment, diagnostic procedures, crisis intervention activities, or standards of care.

10.3 Journaling

HealConnect shall support structured and unstructured journaling activities.

Journaling capabilities shall include:

- Text journaling
- Guided journaling
- Reflection exercises
- Wellness journaling
- Symptom journaling
- Progress journaling
- Voice journaling
- Organization-specific journaling workflows

Journaling functionality is intended to support self-reflection, engagement, continuity activities, communication, monitoring, and information sharing.

Journal content shall contain personal information, consumer health data, PHI, ePHI, clinical information, wellness information, behavioral information, and other sensitive information.

Users are responsible for ensuring journal content is appropriate for its intended purpose.

Journal entries do not constitute diagnoses, treatment plans, prescriptions, clinical recommendations, or professional healthcare services.

10.4 Mood Tracking

Mood tracking functionality shall permit users to document emotional states, self-reported experiences, symptoms, behavioral observations, wellness indicators, subjective perceptions, and related information.

Mood tracking functionality shall support:

- Daily monitoring
- Longitudinal monitoring
- Trend analysis
- Progress visibility
- Care coordination activities
- Outcome tracking

Mood tracking information shall be displayed to authorized providers, care teams, organizations, or authorized personnel when appropriate permissions exist.

Mood tracking information should be interpreted in context and should not be relied upon as a substitute for professional clinical assessment.

10.5 Voice Journaling

HealConnect shall provide voice journaling functionality that enables users to record spoken information for documentation, communication, engagement, continuity-of-care activities, journaling activities, monitoring activities, or related purposes.

Voice journaling shall involve:

- Audio capture
- Audio processing
- Speech recognition
- Voice-to-text conversion
- Summarization
- Organization
- Categorization
- Storage

Voice journaling shall involve AI-assisted processing.

Users are responsible for ensuring compliance with applicable recording laws, consent requirements, privacy obligations, organizational requirements, and legal obligations.

Cognera Health does not determine whether recording activities are legally permissible in a particular jurisdiction.

Users remain solely responsible for compliance with applicable recording requirements.

10.6 Reminders

HealConnect shall provide reminder functionality intended to support engagement, organization, adherence, communication, continuity activities, wellness activities, and care coordination.

Reminders shall include:

- Appointment reminders
- Assessment reminders
- Wellness reminders
- Task reminders
- Medication-related reminders
- Follow-up reminders
- Engagement reminders

Reminder functionality is provided as a convenience feature.

Cognera Health does not guarantee delivery, receipt, timing, accuracy, effectiveness, or availability of reminder functionality.

Users remain responsible for managing appointments, treatment plans, medications, and related activities.

10.7 Notifications

Notification functionality shall be utilized to communicate information regarding platform activity, assessments, reminders, communications, engagement activities, care coordination activities, operational events, or related matters.

Notification delivery shall be affected by:

- Device settings
- Connectivity issues
- Third-party service providers
- Mobile operating systems
- User preferences
- System availability

Notification functionality should not be relied upon for emergency communications.

Notifications are not guaranteed.

10.8 Care Team Communication

HealConnect shall support communication among authorized participants.

Communication functionality shall include:

- Messaging
- Care coordination communication
- Follow-up communication
- Educational communication
- Wellness communication
- Administrative communication

Communication functionality is intended to support coordination and information sharing.

Communication functionality is not intended to replace emergency communication systems, crisis intervention systems, emergency response systems, or urgent medical services.

Users should not rely on messaging functionality during emergencies.

10.9 Progress Tracking

HealConnect shall provide progress tracking functionality intended to support visibility into engagement, activities, assessments, goals, wellness activities, continuity activities, and related information.

Progress tracking shall include:

- Historical views
- Trend visualization
- Assessment tracking
- Goal monitoring
- Outcome monitoring
- Engagement monitoring

Progress tracking information shall be influenced by data quality, user participation, timing, system availability, integrations, and related factors.

Progress tracking information should not be interpreted as guarantees of outcomes.

10.10 Continuity of Care

Continuity-of-care functionality is intended to support ongoing engagement and information sharing between formal encounters.

Continuity-of-care capabilities shall support:

- Follow-up activities
- Monitoring activities
- Crisis identification activites
- Communication activities
- Assessment activities
- Educational activities
- Care coordination activities
- Engagement activities

These functions are intended to supplement—not replace—professional healthcare services.

Continuity-of-care functionality does not establish a duty to monitor users continuously, respond to emergencies, provide crisis intervention services, or guarantee healthcare outcomes.

11. COGNERAAI™

11.1 Overview

CogneraAI™ serves as the artificial intelligence foundation supporting various capabilities throughout the Cognera Health ecosystem.

CogneraAI is intended to assist authorized users through automation, analysis, organization, summarization, workflow support, documentation assistance, information retrieval, trend identification, reporting support, and related activities.

CogneraAI is designed to augment human expertise.

CogneraAI is not intended to replace human judgment, professional expertise, clinical decision-making, operational accountability, regulatory compliance responsibilities, or organizational governance responsibilities.

All AI-generated outputs remain subject to human review, validation, oversight, and accountability requirements.

11.2 AI Foundation

CogneraAI utilizes a combination of technologies that shall include:

- Artificial Intelligence
- Machine Learning
- Natural Language Processing
- Natural Language Understanding
- Predictive Analytics
- Statistical Modeling
- Workflow Automation
- Pattern Recognition
- Recommendation Systems

AI technologies shall evolve over time as technology, regulations, scientific understanding, operational requirements, security considerations, customer requirements, and governance practices evolve.

Cognera Health reserves the right to modify, replace, improve, restrict, or retire AI capabilities as appropriate.

11.3 Natural Language Processing (NLP)

Natural Language Processing technologies shall be utilized to analyze, interpret, organize, summarize, categorize, structure, or process textual information.

NLP capabilities shall support:

- Documentation assistance
- Information extraction
- Text classification
- Trend analysis
- Summarization
- Search functionality
- Workflow automation

NLP functionality is inherently probabilistic and shall produce inaccurate or incomplete results.

Human validation remains required.

11.4 Natural Language Understanding (NLU)

Natural Language Understanding functionality shall be utilized to identify contextual relationships, concepts, themes, intent, sentiment, classifications, patterns, and related information from textual or voice-based inputs.

NLU functionality shall assist in:

- Categorization
- Organization
- Routing
- Workflow support
- Reporting
- Analytics
- Documentation assistance

NLU functionality should not be interpreted as understanding, reasoning, diagnosis, clinical judgment, or professional decision-making.

NLU outputs remain subject to review and validation requirements.

11.5 Summarization

CogneraAI™ shall provide summarization functionality designed to assist authorized users in organizing, condensing, reviewing, understanding, and navigating large volumes of information.

Summarization capabilities shall be applied to:

- Clinical documentation
- Progress notes
- Assessments
- Care plans
- Communications
- Operational reports
- Organizational information
- Voice transcriptions
- Historical records
- Longitudinal information

The purpose of summarization functionality is to improve information accessibility, reduce administrative burden, improve operational efficiency, and support informed review activities.

Summaries generated by AI shall omit information, incorrectly prioritize information, mischaracterize information, misunderstand context, or contain factual inaccuracies.

Summaries are intended solely as informational aids.

AI-generated summaries are not intended to replace review of source materials.

Authorized users remain responsible for reviewing source information when making clinical, operational, legal, regulatory, financial, compliance, or business decisions.

No AI-generated summary should be considered complete, authoritative, or sufficient for decision-making without appropriate review.

11.6 Documentation Assistance

CogneraAI shall provide documentation assistance functionality intended to support administrative efficiency and reduce documentation burden.

Documentation assistance shall include:

- Clinical note drafting
- Session summaries
- Documentation suggestions
- Progress note assistance
- Treatment plan assistance
- Care plan assistance
- Structured data extraction
- Documentation organization
- Documentation formatting

Documentation assistance functionality is intended to assist users in creating documentation more efficiently.

Documentation assistance functionality does not:

- Approve documentation
- Certify documentation
- Validate documentation

- Guarantee documentation accuracy
- Determine clinical appropriateness
- Ensure billing compliance
- Establish legal sufficiency

Users remain solely responsible for:

- Accuracy
- Completeness
- Compliance
- Clinical appropriateness
- Documentation quality
- Regulatory requirements
- Billing requirements
- Record retention requirements

AI-generated documentation must be reviewed and approved before use.

11.7 Predictive Analytics

CogneraAI shall utilize predictive analytics technologies intended to identify patterns, trends, correlations, anomalies, risks, opportunities, utilization indicators, workflow issues, engagement indicators, operational signals, and other informational insights.

Predictive analytics shall support:

- Clinical intelligence
- Operational intelligence
- Organizational intelligence
- Utilization monitoring
- Engagement monitoring
- Risk monitoring
- Outcome monitoring
- Resource planning

Predictive analytics are inherently probabilistic.

Predictions are not guarantees.

Predictions shall be influenced by:

- Data quality
- Data completeness
- Data availability
- Model assumptions
- Operational conditions
- Environmental changes
- Regulatory changes
- Human behavior

Predictions should not be interpreted as factual determinations, diagnoses, treatment recommendations, or guarantees of future events.

Users remain responsible for independent evaluation of predictive outputs.

11.8 Recommendation Generation

CogneraAI shall generate recommendations intended to assist users in identifying potential actions, considerations, follow-up activities, workflow opportunities, documentation opportunities, operational issues, or organizational priorities.

Recommendations shall be based upon:

- Available information
- Historical information
- Statistical relationships
- Configured workflows
- Customer configurations
- Organizational preferences

Recommendations are informational in nature.

Recommendations are not directives.

Recommendations do not replace professional judgment.

Recommendations should be independently reviewed before implementation.

Users remain responsible for determining whether recommendations are appropriate for their specific circumstances.

11.9 Workflow Automation

CogneraAI shall support workflow automation activities intended to improve efficiency, consistency, coordination, organization, communication, reporting, documentation, and operational performance.

Workflow automation shall include:

- Routing
- Task generation
- Notifications
- Escalations
- Scheduling assistance
- Report generation
- Data organization
- Administrative automation

Workflow automation is intended to support human users.

Workflow automation does not transfer responsibility for decisions, actions, approvals, supervision, governance, compliance, or accountability.

Organizations remain responsible for governance and oversight of automated workflows.

11.10 Clinical Intelligence Support

CogneraAI shall provide Clinical Intelligence Support functionality intended to assist authorized users in reviewing, organizing, monitoring, analyzing, and understanding available information.

Clinical Intelligence Support shall include:

- Trend visibility
- Outcome monitoring
- Assessment monitoring
- Longitudinal review
- Documentation review support
- Workflow visibility
- Care coordination support
- Operational support

Clinical Intelligence Support functionality is not intended to diagnose, treat, prescribe, determine standards of care, establish treatment plans, or independently make clinical decisions.

All clinical decisions remain the responsibility of licensed healthcare professionals.

AI-generated clinical insights should be reviewed in conjunction with professional expertise, clinical judgment, organizational policies, patient circumstances, applicable standards of care, and regulatory requirements.

PART III – HEALTHCARE DISCLAIMERS

12. HEALTHCARE TECHNOLOGY PROVIDER NOTICE

12.1 Nature of Services

Cognera Health is a healthcare technology company.

Cognera Health develops, licenses, operates, supports, and maintains software, mobile applications, cloud services, artificial intelligence technologies, analytics services, communication services, documentation support technologies, operational intelligence technologies, enterprise intelligence technologies, and related software services.

The services provided by Cognera Health are technology services.

The services provided by Cognera Health are not healthcare services.

The services provided by Cognera Health are not medical services.

The services provided by Cognera Health are not behavioral health services.

The services provided by Cognera Health are not psychotherapy services.

The services provided by Cognera Health are not psychiatric services.

The services provided by Cognera Health are not crisis intervention services.

The services provided by Cognera Health are not emergency services.

Cognera Health provides technology infrastructure designed to support healthcare organizations, care teams, clinicians, administrators, operational leaders, and authorized users.

12.2 Technology Role

Cognera Health functions as a technology provider.

Technology providers develop tools.

Technology providers do not deliver healthcare services merely by making technology available.

The existence of healthcare-related functionality does not mean that Cognera Health is practicing medicine or providing healthcare services.

Technology functionality shall support:

- Documentation
- Communication
- Coordination
- Reporting
- Analytics
- Workflow management
- Monitoring
- Engagement
- Information organization

These activities remain distinct from professional healthcare services.

12.3 No Healthcare Delivery

The availability of healthcare-related information within the platform does not mean healthcare services are being delivered by Cognera Health.

Healthcare services are provided by healthcare professionals and healthcare organizations.

Healthcare decisions remain the responsibility of healthcare professionals.

Care delivery remains the responsibility of healthcare professionals.

Clinical judgment remains the responsibility of healthcare professionals.

Treatment decisions remain the responsibility of healthcare professionals.

Emergency response remains the responsibility of appropriate emergency responders and healthcare professionals.

Cognera Health does not assume responsibility for healthcare delivery activities.

13. NO PRACTICE OF MEDICINE

Cognera Health does not practice medicine.

Nothing within the platform should be interpreted as the practice of medicine.

The platform does not independently:

- Diagnose diseases
- Diagnose disorders
- Diagnose conditions
- Prescribe treatments
- Prescribe medications
- Develop treatment plans
- Determine standards of care
- Establish medical necessity
- Provide clinical decision-making

Any information generated through the platform is intended solely to support authorized users.

Healthcare professionals remain responsible for medical decision-making.

Medical decisions should never be based solely upon AI-generated information.

Professional judgment must always be exercised.

14. NO PRACTICE OF PSYCHOLOGY

Cognera Health does not practice psychology.

The platform does not provide psychological services.

The platform does not conduct psychological evaluations.

The platform does not independently interpret psychological assessments.

The platform does not establish psychological diagnoses.

The platform does not provide psychological treatment.

Psychological services shall only be provided by appropriately licensed professionals.

Psychological decisions remain the responsibility of licensed professionals.

15. NO PSYCHOTHERAPY SERVICES

Cognera Health does not provide psychotherapy services.

Use of communication tools, engagement tools, journaling tools, assessments, educational content, reminders, notifications, analytics, reporting, or AI-generated content does not create a psychotherapy relationship.

Psychotherapy shall only be provided by qualified professionals operating within applicable legal, regulatory, licensing, and professional requirements.

The platform shall facilitate psychotherapy workflows.

Facilitation of workflows does not constitute delivery of psychotherapy services by Cognera Health.

16. NO PSYCHIATRIC SERVICES

Cognera Health does not provide psychiatric services.

Cognera Health does not employ the platform for the purpose of independently diagnosing psychiatric conditions, prescribing psychiatric medications, establishing psychiatric treatment plans, modifying psychiatric treatment plans, or directing psychiatric care.

The existence of psychiatric-related workflows, documentation tools, assessments, reporting tools, analytics capabilities, AI-assisted features, communication capabilities, care coordination functionality, monitoring functionality, or engagement tools does not constitute psychiatric care by Cognera Health.

Psychiatric services shall only be delivered by appropriately licensed professionals acting within the scope of their licenses, applicable laws, professional obligations, organizational policies, and standards of care.

The platform shall assist authorized users in organizing information, reviewing information, documenting information, coordinating activities, monitoring activities, and facilitating communication.

These activities should not be interpreted as psychiatric diagnosis, psychiatric treatment, psychiatric supervision, psychiatric consultation, psychiatric recommendations, psychiatric prescribing, psychiatric intervention, or psychiatric management by Cognera Health.

All psychiatric decisions remain the responsibility of licensed healthcare professionals.

17. NO MEDICAL DIAGNOSIS

Cognera Health does not diagnose medical conditions.

Cognera Health does not diagnose mental health conditions.

Cognera Health does not diagnose behavioral health conditions.

Cognera Health does not diagnose substance use disorders.

Cognera Health does not diagnose developmental disorders.

Cognera Health does not diagnose neurological conditions.

Cognera Health does not establish clinical diagnoses.

The platform shall collect, organize, display, summarize, analyze, monitor, or report information.

Information processing does not constitute diagnosis.

Information analysis does not constitute diagnosis.

AI-generated observations do not constitute diagnosis.

Assessment results do not constitute diagnosis.

Trend information does not constitute diagnosis.

Predictions do not constitute diagnosis.

Alerts do not constitute diagnosis.

Recommendations do not constitute diagnosis.

Only qualified healthcare professionals shall establish diagnoses.

Users shall not rely exclusively upon platform outputs when making diagnostic determinations.

Diagnostic decisions require professional judgment, clinical evaluation, patient interaction, review of relevant information, and consideration of applicable standards of care.

18. NO MEDICAL TREATMENT

Cognera Health does not provide medical treatment.

Cognera Health does not provide behavioral health treatment.

Cognera Health does not provide psychological treatment.

Cognera Health does not provide psychiatric treatment.

Cognera Health does not provide crisis intervention treatment.

Cognera Health does not independently determine treatment plans.

Cognera Health does not independently modify treatment plans.

Cognera Health does not independently implement treatment interventions.

The platform shall support treatment-related workflows through documentation, monitoring, communication, analytics, reporting, and coordination functionality.

Support for treatment-related workflows does not constitute treatment delivery.

All treatment decisions remain the responsibility of appropriately qualified healthcare professionals.

Authorized users are responsible for evaluating the appropriateness of any actions taken based upon information presented by the platform.

Treatment decisions should never be based solely upon AI-generated outputs.

Professional review and validation remain required.

19. NO PRESCRIBING SERVICES

Cognera Health does not prescribe medications.

Cognera Health does not authorize prescriptions.

Cognera Health does not refill prescriptions.

Cognera Health does not modify prescriptions.

Cognera Health does not determine medication appropriateness.

Cognera Health does not provide pharmaceutical recommendations.

The platform shall contain medication-related information, reminders, educational materials, workflow support, reporting functionality, or documentation support.

Such functionality is informational in nature.

Medication decisions remain exclusively within the authority of appropriately licensed healthcare professionals.

Users remain responsible for independently verifying medication-related information.

20. NO PROVIDER-PATIENT RELATIONSHIP

Use of the platform does not create a provider-patient relationship with Cognera Health.

Use of the platform does not create a therapist-client relationship with Cognera Health.

Use of the platform does not create a psychiatrist-patient relationship with Cognera Health.

Use of the platform does not create a psychologist-patient relationship with Cognera Health.

Use of the platform does not create a counseling relationship with Cognera Health.

Use of the platform does not create a fiduciary healthcare relationship with Cognera Health.

Provider-patient relationships shall exist between users and healthcare professionals or healthcare organizations utilizing the platform.

Such relationships are independent of Cognera Health.

Cognera Health serves solely as a technology provider.

Any healthcare relationship that shall exist is between the individual and the applicable healthcare provider or organization.

21. NO CLINICAL DECISION REPLACEMENT

The platform is not intended to replace professional clinical judgment.

Artificial intelligence functionality is not intended to replace professional clinical judgment.

Documentation assistance is not intended to replace professional clinical judgment.

Predictive analytics are not intended to replace professional clinical judgment.

Clinical intelligence functionality is not intended to replace professional clinical judgment.

Assessment functionality is not intended to replace professional clinical judgment.

Reporting functionality is not intended to replace professional clinical judgment.

Analytics functionality is not intended to replace professional clinical judgment.

Authorized users must independently evaluate all available information before making decisions.

Clinical decisions require consideration of factors that shall not be available to the platform.

Human expertise remains essential.

Professional judgment remains essential.

Independent validation remains essential.

22. PROFESSIONAL JUDGMENT REQUIREMENT

All healthcare decisions require professional judgment.

Professional judgment includes evaluation of:

- Patient-specific circumstances
- Clinical history
- Current presentation
- Risk factors
- Environmental factors
- Treatment history
- Professional standards
- Regulatory requirements
- Organizational requirements

Technology cannot fully replicate professional judgment.

Artificial intelligence cannot fully replicate professional judgment.

Analytics cannot fully replicate professional judgment.

Automation cannot fully replicate professional judgment.

Accordingly, users must exercise independent judgment before relying upon platform information.

Failure to exercise appropriate professional judgment shall result in inappropriate outcomes.

Cognera Health expressly disclaims responsibility for decisions made without appropriate professional review.

23. USER RESPONSIBILITIES

Users are responsible for:

- Maintaining appropriate licenses where required
- Following applicable laws
- Following applicable regulations
- Following organizational policies
- Following professional standards
- Reviewing platform outputs
- Validating AI-generated outputs
- Reviewing documentation
- Maintaining security of accounts
- Protecting credentials
- Obtaining necessary consents
- Verifying information before use
- Exercising professional judgment
- Maintaining appropriate supervision
- Monitoring platform use
- Escalating issues when necessary
- Reporting security concerns
- Reporting privacy concerns
- Reporting safety concerns

Users remain accountable for decisions made using platform information.

The existence of automation, artificial intelligence, analytics, reporting, or workflow support functionality does not transfer responsibility from users to Cognera Health.

PART IV – EMERGENCY SERVICES DISCLAIMER

24. NOT EMERGENCY SERVICES

Cognera Health services are not emergency services.

The platform is not designed, intended, certified, licensed, marketed, or operated as an emergency response system.

The platform should not be used to request emergency assistance.

The platform should not be relied upon during emergencies.

Platform availability shall be affected by:

- Internet connectivity
- Mobile network availability
- Infrastructure failures
- System maintenance
- Security incidents
- Third-party dependencies
- User device limitations

For these and other reasons, the platform is not suitable as an emergency response mechanism.

Users experiencing emergencies should immediately contact appropriate emergency services.

25. NOT CRISIS SERVICES

Cognera Health services are not crisis intervention services.

The platform does not provide:

- Crisis counseling

- Crisis intervention
- Crisis response
- Crisis stabilization
- Emergency mental health services
- Emergency behavioral health services
- Emergency psychiatric services

The platform shall contain communication capabilities, assessments, monitoring functionality, alerts, analytics, AI-generated observations, or engagement functionality.

These capabilities should not be interpreted as crisis intervention services.

Users should not rely on the platform during a crisis situation.

Immediate assistance should be obtained through appropriate emergency resources.

26. NOT SUICIDE PREVENTION SERVICES

Cognera Health services are not suicide prevention services.

The platform is not designed, intended, operated, licensed, staffed, monitored, or maintained as a suicide prevention service.

The platform does not function as:

- A suicide hotline
- A suicide prevention hotline
- A suicide crisis center
- A suicide intervention service
- A suicide response service
- An emergency counseling service
- A behavioral crisis service
- A psychiatric emergency service

The platform may contain assessments, journaling capabilities, communication tools, monitoring capabilities, AI-generated observations, engagement tools, reporting functionality, or analytics functionality.

Such functionality does not constitute suicide prevention services.

The presence of risk indicators, behavioral indicators, symptom indicators, mood indicators, assessment responses, journaling content, communication content, AI-generated observations, predictive analytics, or engagement information does not create

an obligation for Cognera Health to monitor, identify, intervene, respond to, escalate, evaluate, or manage suicide risk.

Users should never rely on the platform as a substitute for emergency assistance.

Individuals experiencing thoughts of self-harm, suicide, violence, or imminent danger should immediately contact emergency services, crisis services, or other appropriate resources.

Organizations utilizing the platform remain responsible for establishing and maintaining their own crisis management protocols, escalation procedures, emergency response processes, supervision processes, and clinical workflows.

26A. NOT A 988 REPLACEMENT

Cognera Health services are not a replacement for the 988 Suicide & Crisis Lifeline.

The platform is not operated, staffed, monitored, certified, licensed, endorsed, or maintained as a crisis hotline, suicide prevention hotline, behavioral health crisis center, emergency counseling service, or 24-hour crisis response service.

The platform does not provide:

- 988 Suicide & Crisis Lifeline services
- Crisis hotline services
- Suicide intervention services
- Emergency behavioral health counseling
- Immediate crisis response
- Real-time crisis assessment
- Emergency psychiatric triage
- Emergency emotional support services
- Immediate emergency intervention

The availability of communication tools, messaging functionality, journaling capabilities, assessments, mood tracking, engagement tools, artificial intelligence features, notifications, alerts, predictive analytics, care coordination tools, or monitoring capabilities does not mean that Cognera Health provides 988-equivalent services.

Users should not rely upon the platform during:

- Suicidal crises

- Self-harm crises
- Behavioral health emergencies
- Psychiatric emergencies
- Severe emotional distress
- Threats of violence
- Situations involving imminent danger
- Situations requiring immediate intervention

Messages, assessments, journal entries, communications, alerts, AI-generated outputs, notifications, or other information submitted through the platform shall not be reviewed immediately and shall never be reviewed in real time.

Platform communications shall experience delays due to:

- Internet connectivity issues
- Mobile device limitations
- System maintenance
- Infrastructure interruptions
- Third-party service disruptions
- User availability
- Organizational workflows
- Human review processes

Because delays shall occur, the platform must not be relied upon to obtain immediate crisis assistance.

If you or another person is:

- Thinking about suicide
- Experiencing thoughts of self-harm
- Experiencing a behavioral health crisis
- Experiencing severe emotional distress
- In immediate danger
- At risk of harming yourself or others

Immediately contact:

- 988 Suicide & Crisis Lifeline (United States)
- 911 Emergency Services
- Local emergency services
- A local crisis response team
- An emergency department
- A qualified healthcare professional

Organizations utilizing the platform remain solely responsible for developing and maintaining crisis management procedures, suicide prevention procedures, emergency escalation workflows, emergency response processes, supervision procedures, risk management protocols, and clinical intervention protocols.

Cognera Health does not assume responsibility for identifying, monitoring, escalating, intervening in, responding to, preventing, managing, or resolving crisis situations.

The responsibility for crisis assessment, suicide risk assessment, emergency intervention, emergency referrals, emergency escalation, and crisis response remains with licensed healthcare professionals, healthcare organizations, emergency responders, crisis response organizations, and appropriate governmental agencies.

Nothing within the platform shall be interpreted as creating a duty on the part of Cognera Health to continuously monitor users, identify crisis situations, intervene in emergencies, prevent self-harm, prevent suicide, prevent violence, dispatch emergency services, or otherwise provide crisis response services.

Users acknowledge and agree that Cognera Health services are intended to support healthcare technology workflows and are not a substitute for 988, emergency services, crisis intervention services, suicide prevention services, or professional emergency assistance.

27. NOT A 911 REPLACEMENT

Cognera Health services are not a substitute for emergency response systems.

The platform is not a replacement for:

- 911
- Emergency medical services
- Police services
- Fire services
- Crisis response teams
- Emergency dispatch centers
- Mobile crisis units
- Emergency departments
- Emergency psychiatric services

Messages sent through the platform shall not be reviewed immediately.

Notifications shall not be delivered immediately.

Assessments shall not be reviewed immediately.

AI-generated outputs shall not be reviewed immediately.

Platform communications shall experience delays due to:

- Internet connectivity issues
- Mobile network disruptions
- System maintenance
- Infrastructure issues
- Third-party service interruptions
- User availability
- Organizational workflows

Because delays shall occur, the platform should never be relied upon to obtain emergency assistance.

Emergency services should be contacted directly through appropriate emergency channels.

28. NOT EMERGENCY DISPATCH

Cognera Health does not provide emergency dispatch services.

Cognera Health personnel do not function as emergency dispatch operators.

Platform systems do not function as emergency dispatch systems.

AI functionality does not function as emergency dispatch functionality.

The platform is not designed to:

- Dispatch police
- Dispatch fire services
- Dispatch emergency medical services
- Dispatch crisis response teams
- Coordinate emergency transportation
- Coordinate emergency evacuations
- Coordinate rescue operations

Users must independently contact appropriate emergency responders when emergency assistance is needed.

Cognera Health assumes no responsibility for delays associated with emergency communications sent through the platform.

29. EMERGENCY ESCALATION RESPONSIBILITIES

Organizations utilizing Cognera Health services are responsible for developing and maintaining appropriate emergency response procedures.

Organizations should establish procedures addressing:

- Suicide risk
- Self-harm risk
- Violence risk
- Abuse reporting
- Crisis intervention
- Emergency referrals
- Emergency escalation
- Emergency communication
- Safety monitoring
- Mandatory reporting obligations

Cognera Health does not establish emergency response protocols on behalf of organizations.

Organizations remain responsible for determining appropriate escalation pathways, clinical workflows, supervision requirements, documentation requirements, and response expectations.

The platform shall facilitate communication and information sharing, but emergency response remains the responsibility of organizations and licensed professionals.

30. USER RESPONSIBILITIES DURING EMERGENCIES

Users experiencing emergencies should immediately seek appropriate assistance.

Users should not:

- Wait for platform responses
- Wait for notifications
- Wait for AI-generated outputs

- Wait for provider messages
- Wait for assessment review
- Wait for documentation review
- Wait for administrative review

Users are responsible for contacting emergency services when immediate assistance is needed.

Users acknowledge that platform availability, connectivity, notifications, messaging systems, and AI functionality cannot be guaranteed.

Users agree that emergency situations require direct engagement with emergency services and qualified professionals.

31. PROVIDER RESPONSIBILITIES DURING EMERGENCIES

Healthcare providers utilizing the platform remain responsible for establishing and implementing appropriate emergency procedures.

Providers remain responsible for:

- Crisis assessment
- Risk assessment
- Escalation decisions
- Mandatory reporting
- Safety planning
- Emergency referrals
- Documentation
- Clinical decision-making
- Compliance obligations

Cognera Health does not assume clinical responsibility for emergency situations.

Providers should maintain independent emergency workflows and should not rely exclusively upon platform functionality when responding to emergencies.

PART V – RESPONSIBLE AI GOVERNANCE PROGRAM

32. RESPONSIBLE AI GOVERNANCE PROGRAM

32.1 Program Purpose

Cognera Health maintains a Responsible AI Governance Program intended to support the safe, ethical, transparent, secure, compliant, accountable, and human-centered use of artificial intelligence technologies.

The Responsible AI Governance Program establishes governance structures, oversight mechanisms, policies, procedures, controls, accountability frameworks, monitoring activities, and continuous improvement activities applicable to AI-enabled functionality throughout the Cognera Health ecosystem.

The objective of the program is to promote trustworthy AI practices while supporting healthcare, behavioral health, wellness, operational, administrative, and organizational activities.

The Responsible AI Governance Program is intended to complement privacy, security, compliance, accessibility, risk management, quality management, and operational governance programs.

32.2 Responsible AI Principles

Cognera Health AI systems are guided by the following principles:

Human-Centered Design

AI should support people rather than replace people.

Technology should augment human expertise and decision-making.

Humans remain accountable for outcomes.

Safety

AI systems should be designed and operated with appropriate safeguards intended to reduce risks to individuals, organizations, and stakeholders.

Accountability

Human accountability must remain clearly established.

AI systems do not assume responsibility for decisions.

Transparency

Users should be informed when AI functionality is utilized.

AI outputs should be identifiable where reasonably feasible.

Privacy

AI systems should operate within established privacy requirements.

Security

AI systems should operate within established security controls.

Fairness

AI systems should be evaluated for fairness, performance consistency, and unintended bias.

Reliability

AI systems should be monitored for quality, performance, and reliability.

Continuous Improvement

AI governance activities should evolve as technologies, regulations, standards, risks, and industry expectations change.

33. GOVERNANCE OBJECTIVES

The Responsible AI Governance Program seeks to:

- Promote safe AI use
- Promote responsible AI use
- Promote transparent AI use
- Promote accountable AI use
- Promote secure AI use
- Promote privacy-preserving AI use
- Promote human oversight
- Reduce operational risk
- Reduce regulatory risk
- Reduce privacy risk
- Reduce security risk
- Reduce bias-related risk

- Improve quality
- Improve governance maturity
- Improve trust

Governance activities are intended to support both innovation and risk management.

Cognera Health recognizes that AI systems shall create benefits as well as risks.

Governance programs seek to manage those risks while preserving appropriate innovation opportunities.

34. GOVERNANCE STRUCTURE

Cognera Health maintains a layered governance structure for AI oversight.

Governance responsibilities shall be distributed across:

- Executive leadership
- Product leadership
- Engineering leadership
- Security leadership
- Privacy leadership
- Compliance leadership
- Clinical advisors
- Risk management personnel
- Operational leadership
- External advisors

The governance structure is intended to ensure that AI activities receive multidisciplinary review and oversight.

Governance activities shall include:

- Policy development
- Risk assessments
- Model reviews
- Performance monitoring
- Change approvals
- Incident reviews
- Compliance reviews
- Security reviews

- Privacy reviews
- Quality reviews

The governance structure shall evolve over time to reflect organizational growth, technological developments, legal requirements, regulatory expectations, customer requirements, and industry practices.

35. AI GOVERNANCE COMMITTEE

35.1 Purpose

Cognera Health maintains an AI Governance Committee responsible for oversight of artificial intelligence activities throughout the organization.

The purpose of the AI Governance Committee is to provide multidisciplinary review, oversight, accountability, risk management, and governance of AI-enabled technologies.

The Committee is intended to ensure that AI systems operate in a manner consistent with:

- Organizational values
- Responsible AI principles
- Privacy requirements
- Security requirements
- Regulatory requirements
- Clinical safety requirements
- Ethical principles
- Customer expectations
- Industry standards

The Committee functions as a governance body rather than an operational decision-making engine.

Final operational responsibilities remain assigned to authorized organizational leaders and personnel.

35.2 Responsibilities

The AI Governance Committee shall oversee:

- AI governance strategy
- AI risk management
- AI policy development

- AI validation activities
- AI monitoring activities
- AI incident reviews
- AI model approvals
- AI model retirement decisions
- AI compliance activities
- AI transparency initiatives
- AI fairness initiatives
- AI accountability initiatives
- AI regulatory monitoring
- AI change management
- AI security reviews
- AI privacy reviews
- AI accessibility reviews

The Committee shall review existing and proposed AI capabilities before deployment or significant modification.

35.3 Membership

Committee membership shall include representatives from:

- Executive leadership
- Product leadership
- Engineering leadership
- Clinical leadership
- Privacy leadership
- Security leadership
- Compliance leadership
- Risk management personnel
- Operational leadership
- Legal leadership
- Accessibility leadership
- External advisors

Membership shall evolve based on organizational growth, regulatory developments, technology changes, customer requirements, and business needs.

36. EXECUTIVE OVERSIGHT

Executive leadership maintains ultimate accountability for organizational AI governance activities.

Executive oversight responsibilities shall include:

- Governance strategy approval
- Resource allocation
- Risk tolerance decisions
- Program oversight
- Policy approval
- Organizational accountability
- Regulatory preparedness
- Strategic direction

Executive oversight helps ensure that AI activities remain aligned with organizational objectives, legal obligations, customer commitments, and governance requirements.

Executive leadership shall receive periodic reporting regarding:

- AI risks
- AI incidents
- AI performance
- AI governance maturity
- Compliance activities
- Monitoring activities
- Regulatory developments

37. CLINICAL OVERSIGHT

Clinical oversight is intended to help ensure that AI-enabled functionality remains aligned with healthcare, behavioral health, wellness, care coordination, and operational objectives.

Clinical oversight activities shall include:

- Review of clinical use cases
- Review of AI-assisted workflows
- Review of clinical recommendations
- Review of documentation workflows

- Evaluation of safety concerns
- Identification of clinical risks
- Validation of intended use
- Escalation of concerns

Clinical oversight does not transfer responsibility for care decisions from licensed professionals to Cognera Health.

Clinical decisions remain the responsibility of healthcare providers.

Clinical oversight is intended to support safe implementation and operation of AI technologies.

38. TECHNICAL OVERSIGHT

Technical oversight is responsible for reviewing the technical design, operation, monitoring, performance, security, resilience, and reliability of AI-enabled technologies.

Technical oversight activities shall include:

- Architecture review
- Design review
- Security review
- Model review
- Monitoring review
- Performance evaluation
- Testing review
- Infrastructure review
- Integration review
- Operational review

Technical oversight personnel shall participate in model approval, deployment reviews, change management processes, incident investigations, and remediation activities.

Technical oversight does not eliminate the need for privacy, security, compliance, clinical, or executive review.

39. COMPLIANCE OVERSIGHT

Compliance oversight is intended to support adherence to applicable legal, contractual, regulatory, accreditation, and governance requirements.

Compliance oversight activities shall include:

- Regulatory monitoring
- Policy review
- Control review
- Documentation review
- Governance review
- Audit preparation
- Audit support
- Corrective action monitoring
- Regulatory risk assessments

Compliance oversight shall consider requirements associated with:

- HIPAA
- HITECH
- GDPR
- UK GDPR
- CCPA
- CPRA
- Consumer health privacy laws
- Telehealth laws
- AI regulations
- Contractual obligations

Compliance oversight does not constitute legal advice and should not be interpreted as a substitute for legal review.

40. PRIVACY OVERSIGHT

Privacy oversight is intended to help ensure that AI-enabled functionality operates in a manner consistent with privacy principles, privacy obligations, contractual requirements, and regulatory requirements.

Privacy oversight activities shall include:

- Privacy impact assessments
- Data flow reviews
- Data minimization reviews
- Consent reviews
- Retention reviews
- De-identification reviews
- Data rights reviews
- Cross-border transfer reviews
- Privacy incident reviews

Privacy oversight supports responsible handling of:

- Personal information
- Consumer health data
- PHI
- ePHI
- Voice data
- Assessment data
- Operational data
- User-generated content

Privacy oversight activities shall be integrated with security, compliance, and governance activities.

41. SECURITY OVERSIGHT

Security oversight is responsible for reviewing security controls applicable to AI-enabled systems and related technologies.

Security oversight activities shall include:

- Threat modeling
- Vulnerability assessments
- Security testing
- Monitoring reviews
- Incident response reviews
- Logging reviews
- Infrastructure reviews
- Access control reviews

- Authentication reviews
- Encryption reviews

Security oversight seeks to reduce risks associated with:

- Unauthorized access
- Data exposure
- Data loss
- System compromise
- Service disruption
- Insider threats
- Third-party risks

Security oversight supports broader organizational security programs.

42. AI RISK MANAGEMENT OVERSIGHT

AI Risk Management Oversight is intended to identify, evaluate, prioritize, monitor, and mitigate risks associated with AI-enabled technologies.

Risk categories shall include:

- Clinical risk
- Privacy risk
- Security risk
- Regulatory risk
- Operational risk
- Reputational risk
- Ethical risk
- Accessibility risk
- Bias risk
- Safety risk

Risk management activities shall include:

- Risk assessments
- Control evaluations
- Risk monitoring
- Risk reporting
- Corrective actions

- Governance reviews

Risk management is a continuous process.

Not all risks can be eliminated.

The objective is responsible management rather than complete elimination of risk.

43. CONTINUOUS MONITORING

Cognera Health maintains monitoring activities intended to support visibility into AI system performance, operational effectiveness, security posture, compliance posture, and governance maturity.

Monitoring activities shall include:

- Model performance monitoring
- Security monitoring
- Logging reviews
- Incident monitoring
- Risk monitoring
- Usage monitoring
- Quality monitoring
- Compliance monitoring
- Operational monitoring

Monitoring activities shall occur continuously, periodically, event-driven, or as otherwise appropriate.

Monitoring outputs shall be used to support investigations, remediation activities, governance reviews, and improvement initiatives.

44. CONTINUOUS IMPROVEMENT

Cognera Health recognizes that AI governance is an evolving discipline.

Technology, regulations, standards, customer expectations, operational requirements, security threats, and privacy requirements continue to change over time.

Accordingly, Cognera Health maintains a commitment to continuous improvement.

Continuous improvement activities shall include:

- Governance reviews
- Policy updates
- Procedure updates
- Risk assessments
- Security enhancements
- Privacy enhancements
- Accessibility enhancements
- Monitoring improvements
- Quality improvements
- AI model improvements
- Regulatory reviews
- Lessons learned reviews

Continuous improvement does not guarantee perfection.

Rather, it reflects an ongoing commitment to responsible governance, accountability, transparency, security, privacy, accessibility, and operational excellence.

PART VI – HUMAN OVERSIGHT FRAMEWORK

45. HUMAN OVERSIGHT FRAMEWORK

45.1 Purpose

Cognera Health maintains a Human Oversight Framework governing the use of AI-enabled functionality throughout the platform.

The purpose of the Human Oversight Framework is to ensure that humans remain responsible for decisions, actions, approvals, judgments, escalations, and outcomes associated with AI-assisted activities.

The Human Oversight Framework recognizes that AI systems shall assist humans but should not replace human accountability.

Human oversight requirements apply regardless of:

- AI model type
- Deployment method
- Use case
- Customer type

- Workflow type
- Organizational configuration

Human oversight requirements are intended to support:

- Safety
- Accountability
- Transparency
- Regulatory compliance
- Professional judgment
- Ethical decision-making
- Risk management
- Quality assurance

The Human Oversight Framework applies across HealScript™, HealConnect™, CogneraAI™, APIs, analytics systems, reporting systems, documentation systems, operational intelligence systems, enterprise intelligence systems, and related technologies.

45.2 Human Accountability Principle

Humans remain accountable.

Artificial intelligence systems do not assume responsibility.

Algorithms do not assume responsibility.

Automation does not assume responsibility.

Models do not assume responsibility.

Technology does not assume responsibility.

Responsibility remains with authorized individuals, organizations, administrators, healthcare professionals, supervisors, and decision-makers.

The use of AI does not transfer accountability to Cognera Health, to the AI system, or to any automated process.

AI is intended to support informed decision-making—not replace it.

46. HUMAN-IN-THE-LOOP

46.1 Purpose

Human-in-the-Loop ("HITL") oversight refers to governance and operational processes requiring direct human participation before AI-generated outputs are accepted, approved, acted upon, finalized, transmitted, documented, implemented, relied upon, or otherwise used.

Human-in-the-Loop controls are intended to ensure that AI systems function as assistive technologies rather than autonomous decision-making systems.

Human-in-the-Loop controls are designed to support:

- Patient safety
- Professional accountability
- Regulatory compliance
- Quality assurance
- Documentation integrity
- Risk management
- Responsible AI use
- Human judgment

Under Human-in-the-Loop requirements, AI outputs remain advisory until reviewed and approved by an appropriately authorized human.

46.2 Human Review Before Action

AI-generated outputs shall not automatically become final decisions.

Appropriate human review shall be required before:

- Clinical use
- Operational use
- Compliance use
- Administrative use
- Financial use
- Billing use
- Reporting use
- Organizational use

Human reviewers remain responsible for determining:

- Accuracy
- Completeness
- Relevance
- Appropriateness
- Compliance
- Safety
- Validity

Approval of an AI-generated output constitutes acceptance of responsibility by the approving individual.

46.3 High-Risk Activities

Human-in-the-Loop controls are particularly important for higher-risk activities.

Examples include:

- Clinical documentation
- Treatment planning
- Care coordination
- Risk assessment
- Safety planning
- Outcome evaluations
- Escalation decisions
- Regulatory reporting
- Compliance decisions
- Operational interventions

AI outputs supporting higher-risk activities should receive enhanced review and validation.

47. HUMAN-ON-THE-LOOP

47.1 Purpose

Human-on-the-Loop ("HOTL") oversight refers to situations where automated systems shall perform certain activities while humans remain responsible for monitoring, supervising, evaluating, and intervening when necessary.

Human-on-the-Loop controls recognize that some activities shall be partially automated while still requiring active human supervision.

The purpose of Human-on-the-Loop oversight is to ensure that:

- Automation remains controlled
- Risks remain visible
- Errors are detected
- Intervention remains possible
- Accountability remains human

47.2 Monitoring Responsibilities

Human supervisors shall monitor:

- AI performance
- Automation performance
- Workflow execution
- Escalation activities
- Alert generation
- Notification delivery
- Data processing activities
- Reporting activities

Monitoring activities shall include both real-time and periodic review.

Human supervisors should maintain sufficient visibility into automated activities to identify unusual conditions, failures, inaccuracies, inappropriate outputs, or unexpected behavior.

47.3 Intervention Authority

Authorized individuals must retain the ability to:

- Override outputs
- Modify outputs
- Correct outputs
- Escalate concerns
- Suspend activities
- Disable functionality

- Stop workflows
- Implement corrective actions

The existence of automation should never prevent appropriate human intervention.

48. HUMAN-OVER-THE-LOOP

48.1 Purpose

Human-over-the-Loop ("HOOTL") oversight refers to governance-level supervision of AI systems, models, workflows, controls, policies, monitoring activities, and operational practices.

Human-over-the-Loop activities occur at the organizational level rather than the individual transaction level.

These activities help ensure that AI systems remain aligned with organizational objectives, legal requirements, regulatory expectations, privacy obligations, security requirements, and ethical principles.

48.2 Governance Responsibilities

Governance-level oversight shall include:

- Policy approval
- Risk review
- Model approval
- Model retirement
- Change approval
- Incident review
- Compliance review
- Security review
- Privacy review
- Quality review

Governance personnel shall evaluate whether AI systems remain appropriate for continued use.

48.3 Independent Oversight

Independent oversight shall be provided by:

- Executive leadership
- Compliance personnel
- Privacy personnel
- Security personnel
- Clinical advisors
- Risk management personnel
- Internal audit personnel
- External advisors

Independent oversight helps reduce the likelihood of unmanaged risks and inappropriate reliance on automation.

49. HUMAN REVIEW REQUIREMENTS

49.1 General Requirement

AI-generated outputs should be reviewed by appropriately qualified individuals before reliance.

The level of review required should be proportionate to:

- Risk level
- Intended use
- Regulatory requirements
- Organizational requirements
- Customer requirements
- Clinical significance

Review activities shall include:

- Accuracy verification
- Completeness verification
- Context review
- Consistency review
- Reasonableness review
- Compliance review
- Quality review

49.2 Qualified Reviewers

Reviews should be conducted by individuals possessing appropriate qualifications, authority, expertise, training, and responsibility.

Qualified reviewers shall include:

- Healthcare professionals
- Clinical supervisors
- Administrators
- Compliance personnel
- Operational personnel
- Subject matter experts

Review authority should be clearly defined.

50. DOCUMENTATION REVIEW REQUIREMENTS

50.1 Documentation Validation

AI-assisted documentation must be reviewed before being finalized.

Review activities shall include:

- Content review
- Accuracy review
- Completeness review
- Consistency review
- Compliance review
- Formatting review
- Billing review
- Regulatory review

AI-generated documentation should never be assumed to be accurate solely because it was generated by technology.

50.2 Documentation Responsibility

The individual approving documentation remains responsible for:

- Accuracy

- Completeness
- Clinical appropriateness
- Regulatory compliance
- Billing compliance
- Record integrity

Approval of documentation constitutes acceptance of responsibility for the content.

51. CLINICAL VALIDATION REQUIREMENTS

51.1 Clinical Review

AI-generated clinical outputs require independent professional evaluation.

Clinical review shall include:

- Clinical relevance
- Clinical appropriateness
- Clinical consistency
- Clinical accuracy
- Patient-specific applicability

Clinical review should consider information not available to the AI system.

51.2 Clinical Decision Authority

Only qualified healthcare professionals may:

- Diagnose conditions
- Develop treatment plans
- Modify treatment plans
- Prescribe medications
- Conduct risk assessments
- Make care decisions

AI systems do not possess clinical authority.

AI outputs must not be interpreted as independent clinical decisions.

51.3 Patient Safety

Patient safety takes precedence over automation efficiency.

Where uncertainty exists:

- Human review should be expanded
- Additional information should be obtained
- Escalation should occur
- Professional judgment should prevail

Safety concerns should always be addressed conservatively.

52. OPERATIONAL VALIDATION REQUIREMENTS

52.1 Operational Review

Operational AI outputs should be validated before implementation when material decisions shall be affected.

Operational validation shall include:

- Data verification
- Trend verification
- KPI validation
- Utilization review
- Resource allocation review
- Workflow review
- Reporting review

Organizations should avoid making significant decisions solely on the basis of unvalidated AI outputs.

52.2 Organizational Impact Review

Where AI outputs shall affect:

- Staffing
- Operations
- Resource allocation
- Performance management

- Compliance activities
- Organizational strategy

additional review shall be appropriate.

Material decisions should involve qualified decision-makers.

53. ESCALATION REQUIREMENTS

53.1 Escalation Triggers

Escalation shall be required when:

- Significant inaccuracies are identified
- Safety concerns arise
- Security concerns arise
- Privacy concerns arise
- Compliance concerns arise
- Regulatory concerns arise
- Model failures occur
- Unexpected behavior occurs
- Material risks are identified

Organizations should maintain documented escalation pathways.

53.2 Escalation Authorities

Escalations shall involve:

- Supervisors
- Clinical leadership
- Security personnel
- Privacy personnel
- Compliance personnel
- Executive leadership
- Risk management personnel

Escalation responsibilities should be clearly assigned.

54. ACCOUNTABILITY REQUIREMENTS

54.1 Human Accountability

Humans remain accountable.

Organizations remain accountable.

Authorized users remain accountable.

Artificial intelligence systems are not accountable entities.

Algorithms are not accountable entities.

Automation systems are not accountable entities.

Technology tools cannot assume legal, professional, ethical, clinical, operational, or regulatory responsibility.

54.2 Decision Accountability

Individuals making decisions based upon AI-supported information remain responsible for those decisions.

Use of AI assistance does not transfer responsibility to:

- Cognera Health
- AI models
- Algorithms
- Automated systems

Decision-makers must exercise independent judgment and maintain accountability for actions taken.

54.3 Governance Accountability

Organizations deploying AI-enabled functionality remain responsible for:

- Governance
- Oversight
- Supervision
- Training
- Compliance

- Risk management
- Policy enforcement
- Quality assurance

Governance accountability cannot be delegated entirely to technology systems.

The use of AI should strengthen human decision-making and governance—not replace it.

PART VII – AI LIMITATIONS

55. HALLUCINATIONS

55.1 General Statement

Artificial Intelligence systems shall generate outputs that appear plausible, authoritative, accurate, complete, professionally written, or otherwise credible while containing information that is inaccurate, fabricated, unsupported, incomplete, outdated, misleading, or incorrect.

These occurrences are commonly referred to as "hallucinations."

Hallucinations shall occur despite the presence of sophisticated models, extensive training data, quality controls, validation processes, governance controls, monitoring activities, and human oversight mechanisms.

The possibility of hallucinations is an inherent limitation of current artificial intelligence technologies.

55.2 Potential Hallucination Risks

Hallucinations shall include:

- Incorrect facts
- Fabricated references
- Incorrect citations
- Incorrect summaries
- Mischaracterized events
- Misinterpreted information
- Incorrect classifications

- Incorrect recommendations
- Incorrect assumptions
- Invented relationships
- Fabricated conclusions
- Unsupported statements

Hallucinations shall occur even when outputs appear highly confident.

The confidence or tone of an AI-generated response should not be interpreted as evidence of accuracy.

55.3 Human Review Requirement

Because hallucinations shall occur, all AI-generated outputs should be independently reviewed before use.

Human review should include evaluation of:

- Accuracy
- Completeness
- Context
- Reasonableness
- Consistency
- Applicability
- Regulatory implications
- Clinical implications

AI-generated outputs should never be accepted solely because they were produced by an AI system.

56. INACCURACIES

56.1 General Statement

Artificial Intelligence systems shall generate inaccurate outputs.

Inaccuracies shall result from:

- Data limitations
- Model limitations

- Incomplete context
- Ambiguous inputs
- Environmental changes
- Regulatory changes
- Technical limitations
- Human factors

Inaccuracies shall range from minor errors to significant errors.

56.2 Sources of Inaccuracy

Inaccuracies shall arise from:

- Misinterpretation of information
- Incorrect assumptions
- Data processing errors
- Classification errors
- Incomplete information
- Ambiguous language
- Outdated information
- Model limitations
- Integration issues

No AI system can guarantee perfect accuracy.

56.3 User Responsibilities

Users remain responsible for validating information before relying upon it.

Independent verification should occur whenever AI outputs are used in support of:

- Clinical decisions
- Operational decisions
- Compliance decisions
- Financial decisions
- Organizational decisions
- Regulatory activities

Human judgment remains essential.

57. BIAS

57.1 General Statement

Artificial Intelligence systems shall exhibit unintended bias.

Bias shall originate from:

- Historical data
- Training data
- Human inputs
- Data collection methods
- Data availability
- Data representation
- System design
- Statistical relationships

Bias shall impact outputs, recommendations, classifications, prioritizations, analyses, summaries, or predictions.

57.2 Potential Effects of Bias

Bias shall result in:

- Uneven performance
- Differential outcomes
- Inaccurate assumptions
- Disproportionate impacts
- Reduced fairness
- Reduced reliability
- Reduced trust

Bias shall affect individuals, groups, organizations, workflows, or populations.

57.3 Bias Monitoring

Cognera Health seeks to monitor AI systems for potential indicators of unintended bias.

Bias monitoring activities shall include:

- Performance reviews
- Validation reviews
- Testing activities
- Quality assessments
- Incident reviews
- Risk assessments

Bias monitoring does not guarantee elimination of all bias.

58. INCOMPLETE CONTEXT

58.1 Context Limitations

AI systems frequently operate using limited information.

The system shall not possess:

- Complete patient history
- Complete organizational history
- Complete operational history
- Real-time circumstances
- Environmental conditions
- Human observations
- Contextual nuances
- Relevant external factors

As a result, AI-generated outputs shall not reflect the full context surrounding a situation.

58.2 Human Context Advantage

Humans possess contextual information that shall not be available to technology systems.

Human reviewers shall understand:

- Organizational culture
- Individual circumstances
- Professional considerations
- Environmental conditions
- Regulatory implications
- Practical realities

AI outputs should therefore be evaluated within the broader context known by human decision-makers.

59. MISSING INFORMATION

59.1 Information Availability

AI systems shall operate using incomplete, unavailable, delayed, corrupted, inconsistent, or missing information.

Missing information shall affect:

- Recommendations
- Predictions
- Analytics
- Summaries
- Documentation
- Reports
- Alerts
- Monitoring outputs

Outputs generated using incomplete information shall be incomplete or inaccurate.

59.2 Reliance Limitations

Users should avoid assuming that AI systems possess all relevant information.

Important information shall be:

- Unavailable
- Delayed
- Not integrated
- Not recorded
- Not accessible
- Not provided

Human review remains necessary to identify missing information and evaluate its significance.

60. MODEL DRIFT

60.1 General Statement

Model drift refers to changes in performance over time caused by changes in data, environments, workflows, populations, operational conditions, technologies, regulations, or other factors.

Model drift shall occur gradually or rapidly.

Model drift is an inherent risk associated with AI systems.

60.2 Causes of Model Drift

Examples include:

- Changes in user behavior
- Changes in workflows
- Changes in healthcare practices
- Changes in regulations
- Changes in technology
- Changes in data sources
- Changes in population characteristics
- Changes in operational conditions

Model performance shall deteriorate if drift is not identified and addressed.

60.3 Monitoring Activities

Cognera Health shall conduct monitoring activities intended to identify indicators of model drift.

Monitoring shall include:

- Performance reviews
- Validation reviews
- Testing
- Quality assurance
- Statistical analysis
- Risk assessments

Monitoring does not guarantee immediate identification of all drift-related issues.

61. PERFORMANCE DEGRADATION

61.1 General Statement

AI performance shall degrade over time.

Performance degradation shall affect:

- Accuracy
- Reliability
- Consistency
- Responsiveness
- Relevance
- Predictive performance
- Classification performance
- Summarization quality

Performance degradation shall occur even when systems continue operating normally.

61.2 Operational Impacts

Performance degradation shall result in:

- Increased errors
- Reduced effectiveness
- Reduced reliability
- Reduced user confidence
- Increased review requirements
- Increased operational risk

Organizations should avoid assuming that historical performance guarantees future performance.

62. REGULATORY CHANGES

62.1 Evolving Regulatory Environment

AI technologies operate within a rapidly evolving regulatory environment.

New laws, regulations, guidance, standards, frameworks, industry practices, and enforcement activities shall emerge over time.

Regulatory changes shall affect:

- AI functionality
- Data processing
- Governance requirements
- Transparency requirements
- Documentation requirements
- Monitoring requirements
- Reporting requirements

62.2 Compliance Implications

Changes in regulatory requirements shall require:

- System modifications
- Policy updates
- Procedure updates
- Workflow changes
- Operational changes
- Additional controls
- Enhanced oversight

Cognera Health reserves the right to modify AI functionality as necessary to support compliance obligations.

63. DATA QUALITY LIMITATIONS

63.1 Importance of Data Quality

AI systems depend upon the quality of data available to them.

Poor-quality data shall negatively affect:

- Accuracy
- Reliability
- Recommendations
- Predictions
- Analytics
- Summaries
- Reporting
- Monitoring

The quality of outputs cannot exceed the quality of inputs.

63.2 Data Quality Risks

Data quality issues shall include:

- Missing information
- Incorrect information
- Inconsistent information
- Duplicate information
- Delayed information
- Corrupted information
- Incomplete records
- Integration errors

Users should evaluate outputs with consideration for underlying data quality.

64. THIRD-PARTY DEPENDENCIES

64.1 Dependency Risks

AI-enabled functionality shall depend upon third-party services, infrastructure, technologies, integrations, APIs, cloud providers, software providers, telecommunications providers, data providers, or other external services.

Performance shall be affected by factors outside the control of Cognera Health.

64.2 Potential Impacts

Third-party issues shall affect:

- Availability
- Reliability
- Performance
- Accuracy
- Security
- Connectivity
- Data access
- Functionality
- Integrations
- User experience

Third-party disruptions shall result in temporary degradation or interruption of services.

64.3 Limitation of Control

Cognera Health does not control all third-party systems.

Accordingly, Cognera Health cannot guarantee uninterrupted performance, availability, accuracy, reliability, or functionality of third-party services.

Users acknowledge that third-party dependencies are an inherent aspect of modern cloud-based technology environments and shall introduce risks beyond the direct control of Cognera Health.

PART VIII – AI TRANSPARENCY

65. USER NOTIFICATION

65.1 Transparency Commitment

Cognera Health is committed to providing reasonable transparency regarding the use of Artificial Intelligence technologies within the platform.

Transparency promotes:

- Trust
- Accountability
- Informed decision-making
- Responsible technology use
- Regulatory compliance
- Ethical deployment
- User awareness

Users should understand when AI functionality shall be involved in generating outputs, supporting workflows, organizing information, producing recommendations, assisting documentation, analyzing information, generating summaries, or performing other AI-assisted activities.

Transparency does not require disclosure of proprietary information, confidential information, trade secrets, security-sensitive information, or intellectual property.

However, Cognera Health seeks to provide sufficient information to allow users to understand the role of AI within the platform.

65.2 AI Use Notifications

Where reasonably feasible and operationally appropriate, Cognera Health shall provide notifications indicating that AI-enabled functionality is being utilized.

Examples shall include:

- AI-generated summaries
- AI-generated documentation
- AI-generated recommendations
- AI-generated classifications

- AI-generated insights
- AI-generated reports
- AI-generated analyses
- AI-generated communications

Notifications shall be provided through:

- User interfaces
- Labels
- Banners
- Icons
- Tooltips
- Documentation
- Product disclosures
- Training materials

The absence of a notification should not be interpreted as evidence that AI was not utilized.

65.3 User Awareness

Users are responsible for understanding the functionality available within the platform.

Organizations are encouraged to provide training and education regarding AI-enabled capabilities.

Authorized users should understand:

- What AI functionality does
- What AI functionality does not do
- Applicable limitations
- Review requirements
- Validation requirements
- Escalation requirements
- Accountability requirements

User awareness supports responsible AI adoption and informed use.

66. OUTPUT LABELING

66.1 AI Output Identification

Cognera Health seeks to identify AI-generated outputs when reasonably feasible and operationally practical.

Output labeling shall assist users in distinguishing between:

- Human-generated content
- AI-generated content
- AI-assisted content
- System-generated content
- User-generated content

Output labeling promotes transparency and supports appropriate review activities.

66.2 Labeling Limitations

Not all outputs can be labeled in every circumstance.

Operational, technical, workflow, integration, security, usability, or organizational considerations shall affect output labeling practices.

Accordingly, users should not assume that unlabeled content was generated solely by humans.

Organizations should maintain awareness that AI functionality shall contribute to outputs throughout the platform.

66.3 Human Review Regardless of Labeling

Whether or not an output is labeled, review requirements remain applicable.

Users remain responsible for:

- Reviewing outputs
- Validating outputs
- Confirming accuracy
- Confirming appropriateness
- Confirming compliance

Labeling does not eliminate review responsibilities.

67. EXPLAINABILITY

67.1 Purpose

Explainability refers to the ability to provide information regarding how outputs were generated, what information influenced outputs, and what limitations shall apply.

Explainability helps users:

- Understand outputs
- Evaluate outputs
- Validate outputs
- Challenge outputs
- Improve trust
- Improve accountability

Cognera Health seeks to support explainability where reasonably feasible.

67.2 Practical Limitations

Certain AI technologies shall operate using highly complex computational processes.

Accordingly, complete explanation of every internal computational process shall not be feasible, practical, understandable, or technically possible.

Explainability should therefore be interpreted as a reasonable effort to provide meaningful information regarding outputs rather than a guarantee of complete technical transparency.

67.3 Explainability Information

Explainability information shall include:

- Source references
- Supporting data
- Confidence indicators
- Relevant factors
- Risk indicators
- Validation requirements

- Limitations
- Contextual information

Explainability information should assist human review rather than replace it.

68. TRACEABILITY

68.1 Purpose

Traceability refers to the ability to identify and reconstruct information regarding AI-related activities.

Traceability supports:

- Governance
- Compliance
- Security
- Incident investigations
- Quality assurance
- Audit activities
- Accountability

Traceability helps organizations understand how outputs were generated and how decisions were reached.

68.2 Traceability Activities

Traceability shall include:

- Input tracking
- Output tracking
- User activity tracking
- Model version tracking
- Workflow tracking
- Approval tracking
- Override tracking
- Escalation tracking
- Review tracking

Traceability activities support operational transparency and accountability.

68.3 Traceability Limitations

Traceability capabilities shall vary depending on:

- Product configuration
- Customer configuration
- Technical architecture
- Legal requirements
- Retention requirements
- Security considerations

Traceability does not guarantee perfect reconstruction of every event or activity.

69. AUDITABILITY

69.1 Purpose

Auditability refers to the ability to review, evaluate, inspect, monitor, and assess activities associated with AI-enabled functionality.

Auditability supports:

- Internal reviews
- Compliance reviews
- Governance reviews
- Security reviews
- Privacy reviews
- Regulatory reviews
- Customer reviews

Auditability promotes accountability and operational transparency.

69.2 Audit Records

Audit-related records shall include:

- User activities
- Access activities
- Review activities
- Approval activities

- Override activities
- Escalation activities
- Model activities
- Administrative activities
- Security activities

Audit records shall be retained according to applicable policies, contracts, regulatory requirements, and operational requirements.

69.3 Audit Limitations

Audit records shall be subject to:

- Retention limitations
- Technical limitations
- Privacy restrictions
- Security restrictions
- Legal restrictions

Auditability should not be interpreted as a guarantee that all historical information will always remain available.

70. DECISION ACCOUNTABILITY

70.1 Human Responsibility

Humans remain accountable for decisions.

Organizations remain accountable for decisions.

Authorized users remain accountable for decisions.

AI systems are not accountable decision-makers.

Technology systems are not accountable decision-makers.

Automation systems are not accountable decision-makers.

Responsibility cannot be delegated to technology.

70.2 Decision-Making Authority

Decision-making authority remains with:

- Healthcare professionals
- Supervisors
- Administrators
- Organizational leaders

• Authorized personnel

Technology shall support decision-making but does not assume authority over decision-making.

70.3 Documentation of Decisions

Organizations shall maintain records documenting:

- Decisions made
- Supporting information
- Reviews conducted
- Approvals provided
- Overrides performed
- Escalations initiated

Documentation supports accountability and governance objectives.

71. AI DOCUMENTATION

71.1 Governance Documentation

Cognera Health shall maintain documentation relating to AI governance activities.

Examples include:

- Policies
- Standards
- Procedures
- Risk assessments
- Validation records
- Monitoring records

- Incident records
- Review records
- Training materials

Documentation supports governance, accountability, transparency, and compliance.

71.2 Operational Documentation

Operational documentation shall include:

• Configuration records

• Change records

• Testing records

• Deployment records

• Review records

• Approval records

• Escalation records

Operational documentation assists with oversight, investigations, audits, and continuous improvement.

71.3 Documentation Maintenance

Documentation shall be reviewed and updated periodically.

Updates shall occur due to:

- Regulatory changes
- Technology changes
- Operational changes
- Security changes
- Governance improvements
- Customer requirements
- Organizational growth

72. AI RECORDS RETENTION

72.1 Retention Objectives

Cognera Health shall retain AI-related records to support:

- Governance
- Compliance
- Security
- Audits
- Investigations
- Incident response
- Risk management
- Operational activities
- Continuous improvement

Retention activities support accountability and traceability objectives.

72.2 Types of Records

Records shall include:

- AI-generated outputs
- Review records
- Validation records
- Approval records
- Override records
- Monitoring records
- Incident records
- Governance records
- Audit records
- Change records

Retention periods shall vary depending upon legal, contractual, regulatory, operational, privacy, and security requirements.

72.3 Secure Retention and Disposal

AI-related records shall be retained using appropriate administrative, technical, and organizational safeguards.

When retention obligations expire, records shall be:

- Deleted
- Destroyed
- Archived
- De-identified
- Anonymized
- Otherwise dispositioned

using approved processes.

Retention and disposal activities shall be conducted in accordance with applicable laws, contractual requirements, privacy obligations, security requirements, and organizational policies.

PART IX – AI MODEL RISK MANAGEMENT

73. MODEL INVENTORY

73.1 Purpose

Cognera Health maintains an AI Model Inventory intended to support governance, accountability, transparency, risk management, compliance, security, privacy, operational oversight, and lifecycle management activities.

The AI Model Inventory serves as the authoritative record of AI-enabled technologies deployed, tested, evaluated, maintained, monitored, retired, or otherwise utilized within the Cognera Health ecosystem.

Maintaining a complete and accurate inventory helps ensure that AI systems remain visible to governance, compliance, privacy, security, operational, and executive oversight functions.

73.2 Inventory Requirements

The Model Inventory shall include:

- Model name
- Model identifier
- Model purpose
- Model owner
- Model sponsor
- Deployment status
- Deployment location
- Risk classification
- Intended use
- Authorized users
- Data sources
- Training methodologies
- Validation status
- Monitoring status
- Retirement status
- Regulatory considerations
- Version information

Inventory records shall be reviewed periodically to ensure completeness and accuracy.

73.3 Risk Classification

AI models shall be categorized according to risk level.

Examples shall include:

Low Risk

Administrative assistance, formatting assistance, organizational support, workflow optimization, and similar activities.

Moderate Risk

Reporting, analytics, summarization, trend visibility, and related informational activities.

High Risk

Clinical intelligence support, risk visibility functions, healthcare workflow support, decision-support activities, and other functions that shall influence significant decisions.

Risk classifications help determine validation requirements, monitoring requirements, governance requirements, and escalation requirements.

74. MODEL VALIDATION

74.1 Purpose

Model validation is intended to provide reasonable assurance that AI systems operate as intended within their defined scope, limitations, and use cases.

Validation activities help evaluate:

- Reliability
- Accuracy
- Performance
- Safety
- Fairness
- Consistency
- Operational suitability
- Regulatory considerations

Validation is a risk-management activity rather than a guarantee of performance.

74.2 Validation Activities

Validation activities shall include:

- Technical reviews
- Functional reviews
- Performance reviews
- Data reviews
- Security reviews
- Privacy reviews
- Compliance reviews
- Clinical reviews
- Risk reviews

- Governance reviews

Validation shall occur before deployment, during deployment, after deployment, and throughout the model lifecycle.

74.3 Validation Limitations

Validation cannot eliminate all risk.

Validation cannot guarantee:

- Perfect accuracy
- Perfect reliability
- Perfect fairness
- Perfect performance
- Absence of hallucinations
- Absence of bias
- Absence of future degradation

Validation provides evidence supporting reasonable confidence rather than certainty.

75. MODEL TESTING

75.1 Testing Objectives

Testing activities are intended to evaluate model behavior under expected and unexpected conditions.

Testing helps identify:

- Errors
- Weaknesses
- Failures
- Inconsistencies
- Security concerns
- Safety concerns
- Performance concerns

Testing shall occur before and after deployment.

75.2 Types of Testing

Testing shall include:

Functional Testing

Evaluation of intended functionality.

Performance Testing

Evaluation of responsiveness and effectiveness.

Security Testing

Evaluation of security-related risks.

Privacy Testing

Evaluation of privacy controls.

Bias Testing

Evaluation of fairness-related concerns.

Safety Testing

Evaluation of safety-related concerns.

Regression Testing

Evaluation following modifications or updates.

75.3 Adversarial Testing

Cognera Health shall perform testing intended to identify vulnerabilities associated with unexpected inputs, malicious inputs, manipulation attempts, prompt abuse, misuse scenarios, or unintended model behavior.

Adversarial testing shall help identify weaknesses before exploitation occurs.

76. MODEL MONITORING

76.1 Purpose

AI models require ongoing monitoring after deployment.

Monitoring helps identify:

- Performance changes
- Drift
- Reliability issues
- Security concerns
- Privacy concerns
- Compliance concerns
- Unexpected behavior

Monitoring supports continuous oversight and continuous improvement activities.

76.2 Monitoring Activities

Monitoring activities shall include:

- Performance metrics
- Quality metrics
- Error rates
- Reliability indicators
- Usage patterns
- Incident trends
- Security indicators
- Compliance indicators
- Risk indicators

Monitoring shall occur continuously, periodically, or event-driven.

76.3 Monitoring Outcomes

Monitoring activities shall result in:

- Investigations
- Remediation

- Revalidation
- Escalation
- Additional testing
- Model modifications
- Model retirement

Monitoring is intended to support responsible operation throughout the model lifecycle.

77. MODEL RETIREMENT

77.1 Retirement Objectives

AI models shall eventually require retirement.

Retirement activities help reduce risks associated with:

- Obsolete models
- Unsupported models
- Non-compliant models
- Underperforming models
- High-risk models
- Inappropriate models

Retirement is a normal component of model lifecycle management.

77.2 Retirement Triggers

Retirement shall occur due to:

- Performance degradation
- Regulatory changes
- Security concerns
- Privacy concerns
- Operational changes
- Technological advancements
- Strategic decisions
- Governance decisions

Retirement decisions shall involve multidisciplinary review.

77.3 Retirement Process

Retirement activities shall include:

- Approval reviews
- Risk assessments
- Migration planning
- Data preservation activities
- Documentation updates
- User communications
- Governance reviews

Retired models should not continue operating without appropriate authorization.

78. CHANGE MANAGEMENT

78.1 Purpose

Changes to AI systems shall introduce risk.

Accordingly, Cognera Health maintains change management processes intended to support controlled implementation of modifications.

Change management helps reduce unintended consequences and improve accountability.

78.2 Types of Changes

Changes shall include:

- Model updates
- Configuration changes
- Data source changes
- Infrastructure changes
- Integration changes
- Security changes
- Workflow changes
- Policy changes

Different change categories shall require different levels of review.

78.3 Change Approval

Depending upon risk, changes shall require review by:

- Product leadership
- Engineering leadership
- Security personnel
- Privacy personnel
- Compliance personnel
- Clinical advisors
- Governance personnel

Approval requirements shall vary according to the nature and impact of the proposed change.

79. BIAS ASSESSMENTS

79.1 Purpose

Bias assessments are intended to identify potential sources of unfairness, disproportionate impacts, or unintended discriminatory outcomes.

Bias assessments support responsible AI governance and risk management objectives.

79.2 Assessment Activities

Bias assessments shall evaluate:

- Input data
- Output behavior
- Population impacts
- Performance consistency
- Error patterns
- Statistical indicators
- Operational impacts

Bias assessments shall occur before deployment and throughout the model lifecycle.

79.3 Limitations

Bias assessments shall reduce risks but cannot guarantee elimination of all bias.

Bias can emerge from complex interactions involving:

- Data
- Users
- Context
- Environment
- Operational practices

Accordingly, continuous monitoring remains important.

80. SAFETY ASSESSMENTS

80.1 Purpose

Safety assessments evaluate whether AI systems shall introduce unacceptable risks to individuals, organizations, operations, workflows, information, or services.

Safety assessments support responsible deployment decisions.

80.2 Safety Review Areas

Safety reviews shall evaluate:

- Clinical impacts
- Operational impacts
- Security impacts
- Privacy impacts
- Accessibility impacts
- Compliance impacts
- Human oversight requirements
- Escalation requirements

Safety assessments shall involve multidisciplinary participation.

80.3 Corrective Actions

Where significant concerns are identified, corrective actions shall include:

- Additional testing
- Additional controls
- Additional monitoring
- Usage restrictions
- Model modifications
- Model retirement

Safety considerations should take priority over convenience or efficiency.

81. QUALITY ASSURANCE

81.1 Purpose

Quality assurance activities are intended to promote consistent, reliable, safe, and appropriate operation of AI-enabled technologies.

Quality assurance supports governance, accountability, and continuous improvement.

81.2 Quality Activities

Quality assurance activities shall include:

- Reviews
- Testing
- Monitoring
- Audits
- Corrective actions
- Preventive actions
- Documentation reviews
- Incident reviews
- Governance reviews

Quality assurance activities shall occur throughout the model lifecycle.

81.3 Continuous Improvement

Quality assurance findings shall be used to support:

- Enhancements
- Remediation
- Process improvements
- Governance improvements
- Training improvements
- Monitoring improvements

Continuous improvement remains a core objective of the quality program.

82. INCIDENT ESCALATION

82.1 Purpose

AI-related incidents should be identified, documented, reviewed, and escalated according to their severity, impact, and risk profile.

Timely escalation supports effective response and risk mitigation.

82.2 Escalation Triggers

Escalation shall occur when:

- Significant inaccuracies are identified
- Model failures occur
- Security concerns arise
- Privacy concerns arise
- Compliance concerns arise
- Safety concerns arise
- Unexpected behavior occurs
- Regulatory concerns arise

Severity classifications shall influence escalation timelines and response activities.

82.3 Incident Response Integration

AI incident escalation shall integrate with:

- Security incident response
- Privacy incident response
- Compliance incident management
- Risk management
- Governance review processes

Appropriate stakeholders should be engaged based on incident characteristics.

83. REGULATORY MONITORING

83.1 Purpose

The regulatory environment governing artificial intelligence continues to evolve.

Cognera Health maintains monitoring activities intended to identify developments that shall affect AI governance, operations, compliance obligations, customer requirements, or platform functionality.

83.2 Monitoring Activities

Regulatory monitoring shall include review of:

- Laws
- Regulations
- Guidance
- Enforcement actions
- Industry standards
- Frameworks
- Best practices
- Emerging requirements

Monitoring activities support proactive governance and compliance planning.

83.3 Governance Response

Where regulatory developments are identified, Cognera Health shall implement:

- Policy updates
- Procedure updates

- Control enhancements
- Documentation updates
- Operational changes
- Technical modifications
- Governance improvements

Regulatory monitoring is intended to support continued alignment with applicable legal and compliance requirements while promoting responsible AI deployment and operation.

PART X – PRIVACY & DATA RIGHTS

84. DATA COLLECTION

84.1 Privacy Commitment

Cognera Health recognizes that privacy is fundamental to trust, healthcare delivery, behavioral health services, wellness programs, operational activities, care coordination activities, and responsible technology practices.

Cognera Health is committed to collecting, processing, storing, transmitting, retaining, sharing, securing, and disposing of information in a manner consistent with applicable legal requirements, contractual obligations, regulatory requirements, privacy principles, and responsible data stewardship practices.

Information collection activities are intended to support legitimate healthcare, operational, security, compliance, administrative, business, continuity-of-care, quality improvement, and technology functions.

Information is not collected for purposes that are inconsistent with disclosed purposes, legal requirements, contractual obligations, or authorized uses.

84.2 Categories of Information Collected

Depending upon the nature of the services utilized, Cognera Health shall collect, receive, create, process, maintain, store, transmit, analyze, or otherwise handle:

Account Information

- Names
- Usernames

- Email addresses
- Phone numbers
- Organization names
- User roles
- Authentication credentials
- Account preferences

Clinical Information

- Assessments
- Clinical notes
- Treatment plans
- Care plans
- Progress notes
- Behavioral health records
- Wellness information
- Outcome measures
- Care coordination records

Consumer Health Data

- Symptoms
- Mood information
- Wellness information
- Health goals
- Health-related preferences
- Self-reported information

Voice Information

- Voice recordings
- Voice journaling
- Voice-to-text inputs
- Audio transcriptions

Technical Information

- Device information
- Browser information
- Operating system information
- IP addresses

- Authentication logs
- Audit logs
- Usage information
- Security logs

Organizational Information

- Operational information
- Workflow information
- Reporting information
- KPI information
- Utilization information
- Administrative information

Collection activities shall vary based upon products, services, integrations, customer configurations, legal requirements, and user interactions.

84.3 Sources of Information

Information shall be obtained from:

- Users
- Customers
- Healthcare providers
- Care teams
- Organizations
- APIs
- Integrations
- Authorized third parties
- Customer systems
- Mobile applications
- Websites
- Communication platforms
- Assessment systems
- Documentation systems

Information shall also be generated through platform activities, operational activities, AI-assisted processes, analytics activities, reporting activities, security activities, and governance activities.

85. DATA USE

85.1 Authorized Uses

Cognera Health shall process information for legitimate purposes including:

- Service delivery
- Care coordination
- Documentation support
- Communication
- Workflow management
- Analytics
- Reporting
- Operational intelligence
- Enterprise intelligence
- Security
- Compliance
- Risk management
- Quality assurance
- Customer support
- System administration
- Regulatory compliance
- Legal obligations

Information processing activities shall be limited to purposes that are lawful, authorized, disclosed, contractually permitted, or otherwise permitted under applicable law.

85.2 AI-Assisted Processing

Information shall be processed through AI-enabled functionality to support:

- Documentation assistance
- Summarization
- Classification
- Analytics
- Reporting
- Trend identification
- Workflow automation
- Recommendation generation

AI processing activities remain subject to governance, privacy, security, compliance, human oversight, validation, and accountability requirements.

86. DATA SHARING

86.1 General Principles

Cognera Health does not sell PHI.

Cognera Health does not sell ePHI.

Cognera Health does not sell identifiable health information.

Cognera Health does not monetize health information through data sales.

Information sharing activities are limited to lawful, authorized, contractually permitted, operationally necessary, or otherwise permitted purposes.

86.2 Categories of Recipients

Information shall be shared with:

Healthcare Providers

Authorized providers involved in care delivery.

Care Teams

Authorized personnel participating in care coordination or operational activities.

Customers

Organizations utilizing Cognera Health services.

Service Providers

Authorized vendors supporting operations.

Cloud Providers

Infrastructure providers supporting platform operations.

Regulators

Government agencies where legally required.

Law Enforcement

Where legally required.

Courts

Pursuant to lawful process.

Successor Organizations

During mergers, acquisitions, restructurings, or similar transactions.

All sharing activities remain subject to applicable safeguards.

87. DATA MINIMIZATION

87.1 Principle

Cognera Health seeks to collect and process only information reasonably necessary to support authorized purposes.

Data minimization helps reduce:

- Privacy risk
- Security risk
- Compliance risk
- Operational risk
- Retention obligations
- Exposure risk

Information collection activities should be proportional to the intended purpose.

87.2 Minimization Controls

Data minimization activities shall include:

- Access restrictions
- Retention controls
- Collection controls
- Sharing controls
- Storage controls
- Review controls
- Governance controls

Data minimization is applied throughout the information lifecycle whenever reasonably feasible.

88. PURPOSE LIMITATION

88.1 Purpose-Based Processing

Information shall be processed only for purposes that are:

- Authorized
- Lawful
- Necessary
- Disclosed
- Contractually permitted
- Operationally justified

Purpose limitation helps ensure that information is not used in ways that exceed reasonable expectations or legal permissions.

88.2 Change of Purpose

Where material changes in processing purposes occur, Cognera Health shall update:

- Privacy notices
- Governance documentation
- Policies
- Procedures
- Customer communications

as appropriate.

89. DATA QUALITY

89.1 Quality Objectives

Cognera Health seeks to maintain information that is:

- Accurate
- Relevant
- Complete
- Timely
- Appropriate

Data quality supports:

- Operational effectiveness
- Privacy compliance
- Security activities
- Reporting accuracy
- Responsible AI use

89.2 User Responsibilities

Users remain responsible for reviewing information they provide and correcting inaccuracies when appropriate.

Data quality is a shared responsibility among users, customers, organizations, providers, and platform administrators.

90. PRIVACY RIGHTS

90.1 General Rights

Depending upon jurisdiction and applicable law, individuals shall possess rights relating to:

- Access
- Correction
- Deletion
- Restriction
- Objection

- Portability
- Consent withdrawal
- Complaint submission

Rights shall vary by jurisdiction.

91. HIPAA RIGHTS

Where HIPAA applies, individuals shall possess rights including:

- Access rights
- Amendment rights
- Accounting of disclosures
- Restrictions requests
- Confidential communications requests

HIPAA rights remain subject to applicable legal exceptions and limitations.

92. GDPR RIGHTS

Where GDPR applies, individuals shall possess rights including:

- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restriction
- Right to Object
- Right to Portability
- Rights related to Automated Decision-Making
- Rights related to Consent Withdrawal

Requests shall be evaluated in accordance with applicable legal requirements.

93. CALIFORNIA RIGHTS

Where applicable, California residents shall possess rights including:

- Right to Know
- Right to Access

- Right to Delete
- Right to Correct
- Right to Limit Use of Sensitive Information
- Right to Non-Discrimination

Rights shall be subject to exceptions permitted by law.

94. CONSUMER HEALTH DATA RIGHTS

Individuals shall possess additional rights under applicable consumer health privacy laws.

Such rights shall include:

- Access
- Deletion
- Withdrawal of Consent
- Disclosure Information
- Correction
- Appeals

Availability of rights shall depend upon jurisdiction and applicable law.

95. CROSS-BORDER TRANSFERS

Information shall be processed, stored, transmitted, backed up, or accessed in jurisdictions outside the individual's location.

Cross-border transfers shall occur where operationally necessary.

Cognera Health shall utilize safeguards including:

- Contractual protections
- Security controls
- Privacy controls
- Regulatory transfer mechanisms

Cross-border transfers remain subject to applicable legal requirements.

96. DATA SUBJECT REQUESTS

Cognera Health shall maintain procedures supporting:

- Access requests
- Deletion requests
- Correction requests
- Restriction requests
- Objection requests
- Portability requests

Requests shall require identity verification.

Requests shall be denied where permitted by law.

97. CONSENT MANAGEMENT

Consent shall be obtained where required by law, regulation, contract, customer requirements, organizational requirements, or operational needs.

Consent activities shall include:

- Collection consent
- Processing consent
- Recording consent
- Communication consent
- Marketing consent
- Research consent

Consent requirements shall vary by jurisdiction and use case.

98. DE-IDENTIFICATION

Cognera Health shall de-identify information in accordance with applicable laws and standards.

De-identification shall involve removal, masking, transformation, aggregation, or other techniques designed to reduce the likelihood that information can be linked to an identifiable individual.

De-identified information shall be utilized for:

- Analytics
- Research
- Quality improvement
- Product improvement
- AI improvement
- Reporting
- Operational purposes

where permitted by law.

99. ANONYMIZATION

Where appropriate, Cognera Health shall anonymize information such that it is no longer reasonably associated with an identifiable individual.

Anonymized information shall be retained and utilized for legitimate organizational purposes where permitted by law.

100. DATA RETENTION

Information shall be retained only as long as necessary to support:

- Clinical requirements
- Operational requirements
- Security requirements
- Compliance requirements
- Legal requirements
- Regulatory requirements
- Contractual requirements
- Business continuity requirements

Retention periods shall vary by information type, jurisdiction, customer requirements, and legal obligations.

101. DATA DELETION

When information is no longer required and retention obligations have expired, information shall be:

- Deleted
- Destroyed
- Archived
- De-identified
- Anonymized
- Otherwise dispositioned

using approved methods.

Deletion activities shall be subject to legal, regulatory, contractual, security, audit, preservation, and litigation requirements.

102. LEGAL HOLDS

Information subject to:

- Litigation
- Regulatory investigations
- Audits
- Preservation obligations
- Legal proceedings

shall be retained beyond normal retention periods.

Legal holds shall suspend ordinary deletion activities.

Legal hold requirements take precedence over routine retention schedules.

103. PRIVACY GOVERNANCE

Cognera Health maintains a privacy governance program intended to support:

- Privacy compliance
- Data protection
- Risk management
- Accountability
- Transparency
- Regulatory compliance
- Continuous improvement

Privacy governance activities shall include:

- Policy development
- Risk assessments
- Privacy impact assessments
- Training
- Monitoring
- Audits
- Incident response
- Corrective actions

Privacy governance is intended to support responsible stewardship of information throughout its lifecycle.

PART XI – SECURITY PROGRAM

104. SECURITY GOVERNANCE

104.1 Purpose

Cognera Health maintains an enterprise information security program designed to support the confidentiality, integrity, availability, resilience, accountability, and protection of information, systems, applications, infrastructure, technologies, services, personnel, and operational processes.

The Information Security Program is intended to support the protection of:

- Personal Information
- Consumer Health Data
- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)
- Confidential Information
- Proprietary Information
- Customer Information
- Operational Information
- Organizational Information
- Intellectual Property

The security program is intended to support compliance with applicable legal, regulatory, contractual, operational, and organizational requirements.

The security program is continuously reviewed and shall evolve in response to changes in technology, risks, threats, regulations, customer expectations, and industry practices.

104.2 Security Objectives

Security objectives include:

Confidentiality

Protecting information from unauthorized access, disclosure, or misuse.

Integrity

Protecting information from unauthorized modification, corruption, destruction, or manipulation.

Availability

Ensuring information and services remain accessible to authorized users when required.

Resilience

Maintaining the ability to withstand, respond to, recover from, and adapt to disruptions.

Accountability

Maintaining appropriate auditability, traceability, monitoring, and oversight.

Continuous Improvement

Maintaining ongoing enhancements to security capabilities, controls, processes, and governance activities.

104.3 Security Governance Structure

Security governance shall include participation from:

- Executive leadership
- Security leadership
- Privacy leadership
- Compliance leadership

- Product leadership
- Engineering leadership
- Risk management personnel
- Operational leadership
- Third-party security providers

Governance activities shall include:

- Policy development
- Risk assessments
- Security reviews
- Incident reviews
- Security monitoring
- Control evaluations
- Audit support
- Continuous improvement activities

105. RISK MANAGEMENT

105.1 Risk Management Program

Cognera Health maintains a risk-based security program.

Risk management activities are intended to identify, assess, prioritize, mitigate, monitor, and manage risks affecting:

- Information
- Systems
- Applications
- Infrastructure
- Personnel
- Operations
- Customers
- Services

Risk management activities shall occur continuously or periodically.

105.2 Risk Categories

Security risks shall include:

- Cybersecurity risks
- Insider threats
- Third-party risks
- Privacy risks
- Operational risks
- Regulatory risks
- Availability risks
- Data protection risks
- Infrastructure risks
- AI-related risks
- Cloud risks
- Physical security risks

Risk evaluations shall consider likelihood, impact, exploitability, detectability, and organizational context.

105.3 Risk Treatment

Risk treatment activities shall include:

- Risk mitigation
- Risk avoidance
- Risk transfer
- Risk acceptance
- Risk monitoring

Not all risks can be eliminated.

The objective of the program is responsible management of risk.

106. ASSET MANAGEMENT

106.1 Asset Identification

Cognera Health seeks to maintain visibility into assets supporting service delivery.

Assets shall include:

- Servers
- Workstations
- Mobile devices
- Cloud resources
- Applications
- Databases
- APIs
- Network devices
- Storage systems
- Security systems
- AI systems

Asset inventories support governance, monitoring, security operations, and risk management activities.

106.2 Asset Classification

Information and technology assets shall be classified according to sensitivity, criticality, regulatory requirements, contractual obligations, and business importance.

Examples include:

- Public
- Internal
- Confidential
- Restricted

Classification activities support appropriate security controls.

107. IDENTITY MANAGEMENT

107.1 Identity Governance

Cognera Health maintains identity management controls intended to ensure that individuals receive appropriate access based upon authorized roles and responsibilities.

Identity management activities shall include:

- User provisioning
- User modification
- User review
- User deprovisioning
- Role management
- Access certification

Identity management supports least privilege and segregation of duties objectives.

107.2 Identity Verification

Appropriate identity verification mechanisms shall be utilized before granting access to systems, applications, information, or services.

Verification methods shall vary depending on:

- Risk level
- User role
- System sensitivity
- Regulatory requirements

108. ACCESS CONTROLS

108.1 Principle of Least Privilege

Access should be limited to the minimum level necessary to perform authorized functions.

Users should not receive access beyond what is reasonably necessary for their responsibilities.

Least privilege reduces exposure and helps limit security risk.

108.2 Role-Based Access Control

Access rights shall be assigned according to roles.

Examples include:

- Clinician
- Administrator
- Supervisor
- Care Coordinator
- Operations Manager
- Compliance Officer
- Security Administrator

Role-based controls support scalable access management.

108.3 Access Reviews

Periodic reviews shall be performed to evaluate:

- User access
- Administrative access
- Privileged access
- Shared access
- Service accounts

Access reviews support ongoing governance and security objectives.

109. AUTHENTICATION

109.1 Authentication Controls

Authentication controls help verify user identity before access is granted.

Authentication methods shall include:

- Passwords
- Multi-factor authentication
- Single sign-on
- Identity federation
- Adaptive authentication

Authentication requirements shall vary based on risk and system sensitivity.

109.2 Multi-Factor Authentication

Where appropriate, multi-factor authentication shall be required.

Factors shall include:

- Something known
- Something possessed
- Something inherent

Multi-factor authentication helps reduce unauthorized access risks.

110. AUTHORIZATION

110.1 Authorization Controls

Authorization determines what actions an authenticated user shall perform.

Authorization controls shall govern:

- Viewing data
- Creating records
- Editing records
- Deleting records
- Administrative activities
- Configuration activities

Authorization decisions shall be based on:

- Roles
- Attributes
- Permissions
- Organizational policies

111. ENCRYPTION

111.1 Encryption Objectives

Encryption is utilized to help protect information against unauthorized access and disclosure.

Encryption shall be applied to:

- Data at rest
- Data in transit
- Backups
- Storage systems
- Communication channels
- Mobile applications

Encryption supports privacy, security, and regulatory requirements.

111.2 Encryption Limitations

Encryption reduces risk but does not eliminate all risk.

Security depends upon multiple controls operating together.

Encryption should be considered one component of a broader security program.

112. LOGGING

112.1 Logging Objectives

Logging supports:

- Monitoring
- Investigations
- Incident response
- Audits
- Compliance
- Accountability

Logs shall capture:

- Access activities
- Administrative activities
- Authentication activities
- Security activities

- Operational activities
- AI activities

112.2 Log Protection

Log information shall be protected against unauthorized access, modification, destruction, or disclosure.

Log retention periods shall vary according to legal, contractual, operational, and regulatory requirements.

113. SECURITY MONITORING

113.1 Monitoring Objectives

Monitoring activities are intended to provide visibility into security-relevant events.

Monitoring shall support:

- Threat detection
- Incident identification
- Operational awareness
- Security investigations
- Compliance monitoring

Monitoring shall be automated, manual, or hybrid.

113.2 Security Events

Examples of monitored events shall include:

- Authentication failures
- Privilege changes
- Administrative activities
- Security alerts
- Network events
- Configuration changes
- Access anomalies

Monitoring does not guarantee detection of all threats or incidents.

114. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

114.1 SIEM Program

Cognera Health shall utilize Security Information and Event Management technologies to support centralized visibility into security-relevant activities.

SIEM capabilities shall support:

- Event collection
- Event correlation
- Alerting
- Investigation
- Monitoring
- Reporting
- Threat detection

SIEM technologies support broader security operations activities.

114.2 Alert Management

Security alerts shall be reviewed, prioritized, investigated, escalated, and resolved according to established procedures.

Alert severity shall influence response requirements and escalation activities.

115. ENDPOINT SECURITY

115.1 Endpoint Protection

Endpoints shall include:

- Workstations
- Laptops
- Mobile devices
- Servers
- Virtual machines

Endpoint security controls shall include:

- Malware protection
- Configuration management

- Monitoring
- Hardening
- Encryption
- Patch management

115.2 Endpoint Governance

Endpoint security supports protection of information and services across distributed environments.

Appropriate controls shall vary based upon risk and operational requirements.

116. VULNERABILITY MANAGEMENT

116.1 Purpose

Cognera Health maintains a Vulnerability Management Program designed to identify, assess, prioritize, remediate, mitigate, monitor, and manage security vulnerabilities that shall affect information, systems, applications, infrastructure, services, personnel, customers, or operations.

The objective of the Vulnerability Management Program is to reduce the likelihood that known weaknesses can be exploited in a manner that negatively impacts confidentiality, integrity, availability, privacy, security, compliance, or operational resilience.

Vulnerability management is a continuous process and forms a critical component of the overall security program.

116.2 Vulnerability Identification

Vulnerabilities shall be identified through:

- Automated scanning
- Manual assessments
- Security testing
- Penetration testing
- Security monitoring
- Vendor notifications
- Threat intelligence

- Security researchers
- Internal reporting
- Third-party reporting

Identification activities shall occur continuously, periodically, or as needed.

116.3 Vulnerability Classification

Vulnerabilities shall be classified according to severity.

Severity ratings shall consider:

- Exploitability
- Likelihood
- Impact
- Data sensitivity
- Exposure
- Availability implications
- Regulatory implications
- Customer impact

Classifications shall include:

- Critical
- High
- Medium
- Low
- Informational

Severity ratings shall influence remediation timelines and escalation requirements.

116.4 Remediation Activities

Remediation activities shall include:

- Patching
- Configuration changes
- Infrastructure changes
- Application updates
- Compensating controls

- Access restrictions
- Monitoring enhancements
- System replacement

Remediation activities shall be prioritized according to risk.

117. PATCH MANAGEMENT

117.1 Purpose

Cognera Health maintains a Patch Management Program intended to reduce exposure to known vulnerabilities through timely implementation of security updates and related maintenance activities.

Patch management helps support:

- Security
- Stability
- Reliability
- Compliance
- Operational resilience

Patch management activities apply to infrastructure, operating systems, applications, services, platforms, endpoints, cloud resources, and related technologies.

117.2 Patch Evaluation

Security updates shall be evaluated according to:

• Severity

• Risk

• Exposure

• Operational impact

• Compatibility

• Testing requirements

• Business impact

Patch evaluation helps ensure updates are applied appropriately while minimizing operational disruption.

117.3 Deployment

Patch deployment activities shall include:

- Testing
- Approval
- Scheduling
- Deployment
- Verification
- Monitoring

Emergency patching activities shall occur where necessary to address elevated risks.

118. SECURE DEVELOPMENT

118.1 Purpose

Cognera Health seeks to incorporate security considerations throughout the software development lifecycle.

Secure development practices help reduce risks associated with vulnerabilities, coding errors, design weaknesses, configuration issues, and security defects.

Security is intended to be integrated into development activities rather than added solely after development is complete.

118.2 Development Controls

Secure development activities shall include:

- Security requirements
- Architecture reviews
- Design reviews
- Code reviews
- Security testing
- Dependency reviews

- Vulnerability scanning
- Change management
- Release management

Development activities shall be adjusted based on risk and system criticality.

118.3 Secure Coding

Development personnel shall be trained regarding secure coding practices.

Secure coding objectives shall include reducing:

- Injection vulnerabilities
- Authentication weaknesses
- Authorization weaknesses
- Data exposure risks
- Configuration weaknesses
- Logic flaws

Secure coding practices contribute to overall security posture.

119. PENETRATION TESTING

119.1 Purpose

Penetration testing is intended to evaluate security controls through simulated attack activities.

Penetration testing shall help identify:

- Vulnerabilities
- Misconfigurations
- Security weaknesses
- Exposure risks
- Control gaps

Penetration testing provides an additional layer of assurance beyond automated scanning.

119.2 Testing Scope

Testing shall include:

- Applications
- APIs
- Infrastructure
- Authentication systems
- Administrative interfaces
- Network environments
- Cloud environments
- Mobile applications

Testing scope shall vary according to risk and operational requirements.

119.3 Remediation

Findings identified through testing shall be:

- Documented
- Prioritized
- Investigated
- Remediated
- Retested

Testing findings shall also inform broader security improvement activities.

120. CLOUD SECURITY

120.1 Cloud Security Objectives

Cognera Health utilizes cloud technologies to support platform operations.

Cloud security activities are intended to protect:

- Infrastructure
- Applications
- Data
- Services
- Integrations

- Operational systems

Cloud environments remain subject to security governance, monitoring, and risk management activities.

120.2 Cloud Security Controls

Controls shall include:

- Access controls
- Encryption
- Monitoring
- Logging
- Network segmentation
- Security reviews
- Vulnerability management
- Backup controls
- Configuration management

Cloud controls shall vary according to architecture and service requirements.

120.3 Shared Responsibility

Cloud environments shall operate under shared responsibility models.

Certain security responsibilities shall be assigned to cloud providers while others remain the responsibility of Cognera Health.

Responsibilities shall vary depending upon services utilized.

121. NETWORK SECURITY

121.1 Purpose

Network security controls are intended to help protect communications, systems, services, and information from unauthorized access, misuse, disruption, modification, or disclosure.

Network security supports confidentiality, integrity, availability, and resilience objectives.

121.2 Network Controls

Network controls shall include:

- Segmentation
- Firewalls
- Monitoring
- Access controls
- Traffic filtering
- Intrusion detection
- Intrusion prevention
- Secure communication channels

Network security controls are evaluated periodically and adjusted as needed.

121.3 Monitoring

Network monitoring activities shall support:

- Threat detection
- Security investigations
- Incident response
- Performance monitoring
- Operational awareness

Monitoring activities do not guarantee detection of all threats.

122. BACKUP & RECOVERY

122.1 Purpose

Cognera Health maintains backup and recovery processes intended to support restoration of information and services following disruption, corruption, failure, or loss.

Backup activities help support:

- Availability
- Resilience
- Business continuity
- Disaster recovery

- Operational recovery

122.2 Backup Activities

Backup activities shall include:

- System backups
- Database backups
- Configuration backups
- Infrastructure backups
- Recovery testing

Backup frequency shall vary depending upon risk, criticality, contractual requirements, and operational needs.

122.3 Recovery Activities

Recovery activities shall include:

- Restoration
- Validation
- Testing
- Verification
- Monitoring

Recovery capabilities are periodically evaluated to support operational readiness.

123. DISASTER RECOVERY

123.1 Purpose

Cognera Health maintains disaster recovery capabilities intended to support restoration of critical services following significant disruptions.

Disruptions shall include:

- Infrastructure failures
- Security incidents
- Natural disasters
- Technology failures

- Service outages
- Environmental events

Disaster recovery activities support operational resilience.

123.2 Recovery Objectives

Recovery planning shall consider:

- Recovery priorities
- Critical services
- Recovery timelines
- Dependencies
- Resource requirements

Recovery objectives shall vary depending upon system criticality.

124. BUSINESS CONTINUITY

124.1 Purpose

Business continuity planning is intended to support continued operation of critical functions during disruptions.

Business continuity planning shall address:

- Personnel disruptions
- Technology disruptions
- Infrastructure disruptions
- Security incidents
- Vendor disruptions
- Environmental events

Continuity planning supports organizational resilience.

124.2 Continuity Activities

Activities shall include:

- Risk assessments

- Recovery planning
- Scenario planning
- Testing
- Exercises
- Improvement activities

Business continuity planning shall be reviewed periodically.

125. VENDOR RISK MANAGEMENT

125.1 Purpose

Cognera Health shall utilize third-party vendors, service providers, cloud providers, infrastructure providers, software providers, consultants, contractors, and subcontractors.

Vendor risk management activities help evaluate and manage risks associated with third-party relationships.

125.2 Due Diligence

Vendor evaluations shall consider:

- Security practices
- Privacy practices
- Compliance posture
- Operational resilience
- Service capabilities
- Contractual obligations
- Risk profile

Due diligence activities shall occur before engagement and throughout the relationship lifecycle.

125.3 Ongoing Monitoring

Vendor monitoring shall include:

- Security reviews
- Performance reviews
- Compliance reviews
- Contract reviews
- Risk assessments

Monitoring activities help support ongoing risk management objectives.

126. SECURITY AWARENESS & TRAINING

126.1 Purpose

Security awareness activities help personnel understand their responsibilities regarding privacy, security, compliance, acceptable use, incident reporting, and risk management.

Human behavior remains an important component of security.

Training supports informed and responsible conduct.

126.2 Training Topics

Training shall address:

- Security awareness
- Privacy requirements
- HIPAA obligations
- Incident reporting
- Phishing awareness
- Access management
- Acceptable use
- Data protection
- AI governance
- Regulatory obligations

Training shall occur periodically and shall be supplemented by awareness initiatives.

127. INCIDENT RESPONSE

127.1 Purpose

Cognera Health maintains an Incident Response Program intended to support identification, investigation, containment, eradication, recovery, communication, documentation, and post-incident review activities.

The Incident Response Program supports timely and coordinated management of security incidents.

127.2 Incident Lifecycle

Incident response activities shall include:

Detection

Identification of potential security events.

Analysis

Evaluation of incident characteristics and impact.

Containment

Limiting ongoing impact.

Eradication

Removal of root causes where appropriate.

Recovery

Restoration of normal operations.

Lessons Learned

Review and improvement activities following incident resolution.

127.3 Incident Categories

Incidents shall include:

- Unauthorized access
- Data exposure

- Malware events
- Service disruptions
- Insider threats
- Infrastructure failures
- Third-party incidents
- AI-related incidents

Incident categories shall influence response activities and escalation requirements.

127.4 Regulatory Notification

Where required by law, regulation, contract, or customer obligation, Cognera Health shall provide notifications regarding qualifying incidents.

Notification activities shall be conducted in accordance with applicable:

- HIPAA requirements
- HITECH requirements
- GDPR requirements
- State breach notification laws
- Contractual obligations

Notification timelines and obligations shall vary depending upon applicable requirements.

127.5 Continuous Improvement

Incident response activities shall result in:

- Corrective actions
- Preventive actions
- Policy updates
- Procedure updates
- Training updates
- Security enhancements
- Governance improvements

Lessons learned support ongoing enhancement of the Information Security Program and broader organizational resilience efforts.

PART XII – VULNERABILITY DISCLOSURE PROGRAM

128. RESPONSIBLE DISCLOSURE

128.1 Purpose

Cognera Health™ supports and encourages responsible security research conducted in good faith.

The purpose of this Vulnerability Disclosure Program is to provide a structured process through which security researchers, customers, partners, users, vendors, and other parties shall report potential security vulnerabilities affecting Cognera Health products, services, applications, infrastructure, websites, APIs, integrations, mobile applications, cloud environments, and related technologies.

Cognera Health recognizes that responsible security research contributes to:

- Security improvement
- Risk reduction
- Customer protection
- Privacy protection
- Platform resilience
- Transparency
- Trust
- Continuous improvement

Security research conducted in accordance with this Program is viewed as a valuable component of the organization's overall security strategy.

128.2 Good Faith Expectations

Cognera Health encourages security research that is conducted in good faith.

Good faith activities generally include:

- Identifying vulnerabilities
- Validating vulnerabilities
- Reporting vulnerabilities
- Supporting remediation efforts
- Participating in coordinated disclosure

Researchers are expected to avoid activities that could negatively affect customers, users, healthcare organizations, systems, services, infrastructure, or operations.

128.3 Program Objectives

The Vulnerability Disclosure Program seeks to:

- Improve security
- Reduce risk
- Encourage responsible reporting
- Support coordinated remediation
- Improve transparency
- Facilitate communication
- Protect customers
- Protect users
- Protect healthcare organizations

The Program is intended to supplement—not replace—internal security monitoring, testing, and governance activities.

129. SAFE HARBOR

129.1 Good Faith Research

Cognera Health recognizes the importance of responsible vulnerability disclosure.

Subject to applicable law, researchers who act in good faith and comply with this Program shall be eligible for Safe Harbor protections.

Safe Harbor considerations shall apply where researchers:

- Avoid causing harm
- Avoid accessing unnecessary information
- Avoid service disruption
- Avoid privacy violations
- Avoid destructive activities
- Promptly report findings
- Cooperate during investigations

The intent of Safe Harbor is to encourage responsible reporting rather than discourage security research.

129.2 Limitations

Safe Harbor does not authorize:

- Data theft
- Extortion
- Social engineering
- Physical intrusion
- Service disruption
- Malware deployment
- Privacy violations
- Regulatory violations
- Criminal activity

Safe Harbor does not override applicable laws, contractual obligations, court orders, regulatory requirements, or governmental directives.

129.3 Unauthorized Activities

Activities outside the scope of this Program shall not qualify for Safe Harbor protections.

Examples include:

- Accessing customer data
- Accessing PHI
- Accessing ePHI
- Modifying information
- Deleting information
- Disrupting services
- Exfiltrating information
- Deploying malicious code
- Interfering with operations

Researchers should exercise caution and avoid unnecessary access or impact.

130. REPORTING REQUIREMENTS

130.1 Report Content

Vulnerability reports should contain sufficient information to support investigation and validation.

Reports should include, where applicable:

- Description of vulnerability
- Affected system
- Affected functionality
- Potential impact
- Steps to reproduce
- Supporting evidence
- Screenshots
- Logs
- Proof-of-concept information
- Suggested remediation

The quality and completeness of reports shall affect investigation efficiency.

130.2 Report Accuracy

Researchers should make reasonable efforts to ensure reports are accurate.

Speculative claims, unsupported conclusions, or intentionally misleading information shall delay investigations.

Cognera Health reserves the right to independently validate reported findings.

131. SUBMISSION PROCEDURES

131.1 Reporting Channels

Vulnerability reports shall be submitted through approved communication channels.

Examples shall include:

- security@cogneraheath.ai
- Designated security portals
- Approved reporting mechanisms

Cognera Health shall establish additional reporting methods from time to time.

131.2 Submission Expectations

Reports should be submitted as promptly as reasonably possible after discovery.

Timely reporting supports:

- Risk reduction
- Remediation
- Customer protection
- Coordinated disclosure
- Operational resilience

Researchers should avoid unnecessary delays.

131.3 Communication

Cognera Health shall communicate with researchers regarding:

- Validation
- Clarification
- Investigation status
- Remediation status

• Disclosure coordination

Communication timelines shall vary depending upon:

- Severity
- Complexity
- Operational impact
- Resource availability

132. INVESTIGATION PROCESS

132.1 Initial Review

Reported vulnerabilities shall undergo an initial review process.

Initial review activities shall include:

- Intake
- Triage
- Prioritization
- Classification
- Assignment

Not all reports will ultimately be determined to represent valid vulnerabilities.

132.2 Validation

Validation activities shall include:

- Technical review
- Reproduction
- Security testing
- Risk assessment
- Impact evaluation

Validation helps determine whether a reported issue represents a legitimate security concern.

132.3 Investigation

Investigations shall involve:

- Security personnel
- Engineering personnel
- Product personnel
- Infrastructure personnel
- Compliance personnel
- Privacy personnel
- External experts

Investigations shall vary based upon complexity and severity.

133. SEVERITY RATINGS

133.1 Purpose

Severity ratings help prioritize remediation efforts and response activities.

Severity ratings shall consider:

- Likelihood
- Impact
- Exploitability
- Exposure
- Data sensitivity
- Customer impact
- Operational impact

133.2 Critical Severity

Critical vulnerabilities shall involve:

- Unauthorized access to regulated data
- Remote code execution
- Significant privilege escalation
- System compromise
- Major security failures

Critical findings generally receive the highest remediation priority.

133.3 High Severity

High severity findings shall involve:

- Significant security weaknesses
- Elevated access risks
- Significant confidentiality concerns
- Significant integrity concerns

High severity findings shall require accelerated remediation.

133.4 Medium Severity

Medium severity findings shall involve:

- Moderate security concerns
- Limited exposure
- Limited operational impact

Medium severity findings remain important and should be addressed appropriately.

133.5 Low Severity

Low severity findings shall include:

- Minor weaknesses
- Limited exploitability
- Limited exposure
- Informational concerns

Low severity findings shall still contribute to broader security improvements.

134. REMEDIATION LIFECYCLE

134.1 Remediation Objectives

Cognera Health seeks to address validated vulnerabilities in a risk-based manner.

Remediation activities shall include:

- Patching
- Configuration changes
- Infrastructure updates
- Code changes
- Process improvements
- Monitoring enhancements
- Compensating controls

The remediation approach shall vary according to the nature of the issue.

134.2 Verification

Following remediation, validation activities shall be conducted to confirm effectiveness.

Verification activities shall include:

- Testing
- Retesting
- Security reviews
- Monitoring

Verification helps ensure remediation objectives have been achieved.

134.3 Closure

Issues shall be considered closed after:

- Investigation
- Remediation
- Verification
- Documentation
- Approval

Closure does not prevent future monitoring or reassessment.

135. COORDINATED DISCLOSURE

135.1 Purpose

Cognera Health supports coordinated vulnerability disclosure practices.

Coordinated disclosure allows vulnerabilities to be remediated before widespread public disclosure.

This approach helps reduce risk to:

- Customers
- Users
- Healthcare organizations
- Services
- Infrastructure

135.2 Disclosure Coordination

Cognera Health shall work collaboratively with researchers regarding:

- Disclosure timing
- Public communications
- Technical details
- Remediation status

Coordinated disclosure timelines shall vary according to risk and operational considerations.

135.3 Public Disclosure

Researchers are encouraged to avoid public disclosure until remediation activities have been completed or otherwise coordinated.

Premature disclosure shall increase risks to customers and users.

136. RESEARCHER RECOGNITION

136.1 Appreciation

Cognera Health appreciates responsible security research conducted in good faith.

Responsible reporting contributes to stronger security and improved protection for customers and users.

136.2 Recognition Programs

At its discretion, Cognera Health shall recognize researchers through:

- Acknowledgements
- Hall of Fame listings
- Recognition programs
- Security communications

Recognition is not guaranteed.

Recognition criteria shall change over time.

136.3 No Obligation

Unless otherwise agreed in writing, vulnerability submissions do not create any obligation to provide compensation, rewards, employment opportunities, partnerships, or other benefits.

137. SECURITY COMMUNICATIONS

137.1 Security Notifications

Cognera Health shall issue security communications relating to:

- Vulnerabilities
- Security advisories
- Security updates
- Security enhancements
- Risk notifications
- Remediation guidance

Communications shall be provided through appropriate channels.

137.2 Customer Communications

Customers shall receive communications regarding security matters where appropriate.

Communications shall include:

- Advisory information
- Risk information
- Remediation information
- Required actions
- Recommended actions

Communication timing shall depend upon operational, legal, regulatory, privacy, and security considerations.

137.3 Continuous Improvement

Lessons learned from vulnerability disclosures shall be incorporated into:

- Security governance
- Risk management
- Secure development
- Testing programs
- Monitoring programs
- Incident response
- Training programs
- Policies and procedures

The Vulnerability Disclosure Program is intended to support continuous enhancement of the overall Information Security Program and organizational resilience.

PART XIII – ACCESSIBILITY & INCLUSIVE DESIGN

138. ACCESSIBILITY GOVERNANCE

138.1 Purpose

Cognera Health™ is committed to designing, developing, maintaining, and improving products, services, technologies, content, and digital experiences that are accessible, inclusive, usable, and equitable for all individuals, including individuals with disabilities.

Accessibility is a core component of product quality, user experience, risk management, compliance, responsible technology development, and organizational governance.

The purpose of the Accessibility Governance Program is to establish the principles, responsibilities, controls, processes, oversight activities, monitoring activities, and continuous improvement mechanisms supporting accessibility throughout the Cognera Health ecosystem.

Accessibility governance supports:

- Equal access
- Usability
- Inclusion
- Compliance
- User experience

- Risk management
- Continuous improvement
- Responsible innovation

Accessibility governance is intended to be integrated throughout the product lifecycle rather than treated as a separate activity.

138.2 Governance Responsibilities

Accessibility governance responsibilities shall be distributed across:

- Executive leadership
- Product leadership
- Engineering leadership
- Design teams
- Quality assurance teams
- Compliance personnel
- Legal personnel
- Accessibility specialists
- Customer support personnel
- External advisors

Accessibility responsibilities shall include:

- Policy development
- Design review
- Accessibility testing
- Issue management
- User feedback review
- Remediation planning
- Continuous improvement activities

Accessibility governance is intended to support organization-wide accountability.

139. ACCESSIBILITY PROGRAM OBJECTIVES

139.1 Program Goals

Cognera Health seeks to provide digital experiences that are:

- Perceivable
- Operable
- Understandable
- Robust
- Inclusive
- Accessible
- User-friendly
- Consistent

Accessibility objectives support individuals with a broad range of needs and abilities.

139.2 Accessibility Outcomes

Accessibility initiatives are intended to:

- Reduce barriers
- Improve usability
- Improve user experience
- Increase participation
- Support equitable access
- Enhance customer satisfaction
- Improve operational effectiveness

Accessibility improvements benefit all users, not solely users with disabilities.

139.3 Organizational Commitment

Cognera Health views accessibility as an ongoing commitment rather than a one-time project.

Accessibility requirements, technologies, standards, regulations, and user expectations continue to evolve.

Accordingly, accessibility governance is intended to support continuous enhancement of products and services over time.

140. ADA COMMITMENT

140.1 Accessibility Commitment

Cognera Health is committed to supporting accessibility principles reflected in the Americans with Disabilities Act ("ADA").

Accessibility considerations are incorporated into product development, content development, governance activities, quality assurance activities, support activities, and continuous improvement efforts.

The organization seeks to reduce unnecessary barriers to access whenever reasonably feasible.

140.2 Equal Access Objectives

Cognera Health seeks to provide individuals with meaningful access to digital services regardless of disability status.

Accessibility efforts shall support individuals with:

- Visual impairments
- Hearing impairments
- Mobility impairments
- Cognitive impairments
- Neurological conditions
- Learning disabilities
- Temporary impairments
- Age-related limitations

Accessibility efforts are intended to improve usability for a diverse range of users.

140.3 Continuous Evaluation

ADA-related accessibility efforts are reviewed periodically and shall be adjusted as technology, legal requirements, accessibility standards, customer expectations, and operational requirements evolve.

141. WCAG 2.2 ALIGNMENT

141.1 Accessibility Standards

Cognera Health seeks to align accessibility efforts with Web Content Accessibility Guidelines (WCAG) 2.2 where reasonably applicable.

WCAG serves as an internationally recognized framework for digital accessibility.

Accessibility initiatives shall be informed by WCAG principles including:

- Perceivable
- Operable
- Understandable
- Robust

141.2 Implementation Considerations

WCAG alignment shall include efforts relating to:

- Keyboard navigation
- Alternative text
- Color contrast
- Focus indicators
- Error identification
- Form accessibility
- Screen reader compatibility
- Accessible structure

Implementation approaches shall vary depending on technology, architecture, platform, operational requirements, and product capabilities.

141.3 Practical Limitations

Complete conformity shall not be achievable in all circumstances.

Accessibility initiatives are implemented using a risk-based and continuous improvement approach.

Accessibility objectives should be interpreted as ongoing commitments rather than guarantees of perfect accessibility in every circumstance.

142. SECTION 508 ALIGNMENT

142.1 Federal Accessibility Principles

Where appropriate, Cognera Health shall consider accessibility principles reflected in Section 508 of the Rehabilitation Act.

Section 508 considerations shall be relevant for:

- Government customers
- Educational organizations
- Public sector entities
- Accessibility-focused procurement activities

Accessibility efforts shall incorporate practices that support Section 508-related objectives.

142.2 Accessibility Reviews

Accessibility evaluations shall consider:

- User interfaces
- Content
- Forms
- Navigation
- Documentation
- Reports
- Mobile applications
- Web applications

Review methodologies shall evolve over time.

143. ACCESSIBLE PRODUCT DESIGN

143.1 Design Philosophy

Accessibility considerations are intended to be incorporated during product design activities whenever reasonably feasible.

Accessible design shall include consideration of:

- Usability
- Readability
- Navigation
- Interaction design
- Error handling
- Cognitive load
- User workflows

Accessibility is considered alongside privacy, security, compliance, performance, and operational requirements.

143.2 Inclusive Design

Inclusive design seeks to recognize the diverse needs of users.

Design activities shall consider:

- Different abilities
- Different devices
- Different environments
- Different interaction methods
- Different learning styles

Inclusive design contributes to broader accessibility objectives.

144. ACCESSIBILITY TESTING PROGRAM

144.1 Purpose

Accessibility testing helps identify barriers affecting usability and accessibility.

Testing activities support remediation, quality assurance, governance, and continuous improvement efforts.

144.2 Testing Activities

Testing shall include:

- Automated testing
- Manual testing
- Screen reader testing
- Keyboard navigation testing
- Mobile accessibility testing
- Browser compatibility testing
- Accessibility reviews

Testing approaches shall vary depending upon technology and risk.

144.3 Testing Limitations

Testing cannot guarantee identification of all accessibility issues.

Accordingly, accessibility testing is complemented by reviews, monitoring, feedback, and continuous improvement activities.

145. ACCESSIBILITY REVIEWS

145.1 Review Activities

Accessibility reviews shall occur:

- During design
- During development
- Before release
- After release
- During updates
- During audits

Review activities support early identification of potential accessibility concerns.

145.2 Review Criteria

Reviews shall consider:

- Accessibility standards
- Usability principles
- User experience
- Accessibility feedback
- Technical feasibility

Review outcomes shall inform remediation priorities.

146. ACCESSIBILITY ISSUE MANAGEMENT

146.1 Identification

Accessibility issues shall be identified through:

- Testing
- Audits
- Monitoring
- User feedback
- Customer feedback
- Support requests
- Internal reviews

Accessibility concerns are evaluated according to risk, impact, severity, and feasibility.

146.2 Remediation

Remediation activities shall include:

- Design updates
- Content updates
- Development changes
- Workflow improvements
- Documentation improvements

Remediation priorities shall be based on severity and user impact.

147. ACCESSIBILITY ROADMAP

147.1 Continuous Improvement Planning

Cognera Health shall maintain accessibility improvement initiatives intended to enhance accessibility over time.

Roadmap activities shall include:

- Accessibility enhancements
- Process improvements
- Training improvements
- Testing improvements
- Governance improvements

Roadmaps shall evolve based on organizational priorities and user needs.

148. USER FEEDBACK

148.1 Feedback Program

User feedback is an important component of accessibility governance.

Feedback shall help identify barriers, usability concerns, improvement opportunities, and accessibility priorities.

148.2 Feedback Channels

Feedback shall be submitted through:

- Support channels
- Accessibility contact channels
- Customer communications
- User requests

Feedback shall be reviewed and prioritized according to established processes.

149. ACCOMMODATION REQUESTS

149.1 Accessibility Assistance

Individuals experiencing accessibility barriers shall request assistance.

Cognera Health seeks to make reasonable efforts to address accessibility concerns and provide appropriate accommodations where feasible.

149.2 Evaluation Process

Accommodation requests shall be reviewed based upon:

- Nature of the issue
- Technical feasibility
- Operational considerations
- Accessibility requirements

Requests shall result in remediation activities, alternative access methods, or other reasonable accommodations.

150. THIRD-PARTY ACCESSIBILITY

150.1 Third-Party Technologies

Cognera Health services shall integrate with or depend upon third-party technologies.

Third-party technologies shall include:

- Cloud services
- Communication services
- Analytics services
- Identity services

• Embedded content

Cognera Health does not control all aspects of third-party accessibility.

150.2 Vendor Considerations

Where appropriate, accessibility considerations shall be incorporated into vendor evaluation activities.

However, Cognera Health cannot guarantee accessibility characteristics of third-party products or services.

151. CONTINUOUS IMPROVEMENT

151.1 Commitment

Accessibility is an ongoing process.

Cognera Health is committed to continually evaluating and improving accessibility practices.

Continuous improvement activities shall include:

- Accessibility reviews
- Governance reviews
- Training
- Testing
- Remediation
- User engagement
- Monitoring
- Process enhancements

151.2 Future Enhancements

Accessibility standards, technologies, expectations, and regulations continue to evolve.

Cognera Health intends to adapt accessibility practices as appropriate to support evolving accessibility objectives, user needs, technological developments, and legal requirements.

Accessibility improvement should be viewed as a continuing organizational commitment rather than a one-time activity.

151.3 Accessibility Contact

Accessibility inquiries, feedback, accommodation requests, and accessibility-related concerns shall be directed to:

accessibility@cognerahealth.ai

Cognera Health, Inc.

Accessibility-related communications shall be reviewed and addressed through established governance, support, and continuous improvement processes.

PART XIV – INTELLECTUAL PROPERTY & PROPRIETARY RIGHTS

152. INTELLECTUAL PROPERTY OVERVIEW

152.1 Purpose

The purpose of this section is to define ownership, protection, use, licensing, restrictions, and governance requirements relating to the intellectual property, proprietary technology, software, artificial intelligence systems, algorithms, content, trademarks, documentation, and related assets of Cognera Health™.

Intellectual Property represents one of the organization's most valuable assets and includes technology, software, inventions, methodologies, business processes, designs, documentation, data structures, models, frameworks, workflows, interfaces, trade secrets, and other proprietary materials developed, acquired, licensed, maintained, or controlled by Cognera Health.

The protections described in this section are intended to preserve:

- Innovation
- Competitive advantage
- Trade secrets
- Confidential information
- Software assets
- Brand assets
- Customer trust
- Technology investments

Nothing in this Framework shall be interpreted as transferring ownership of Cognera Health intellectual property unless expressly stated in a separate written agreement.

153. TRADEMARKS

153.1 Ownership of Trademarks

Cognera Health owns or licenses various trademarks, service marks, trade names, logos, branding elements, slogans, product names, design marks, visual identifiers, and related intellectual property.

Examples shall include:

- Cognera Health™
- HealScript™
- HealConnect™
- CogneraAI™
- Cognitive and Collaborative Intelligence™
- Associated logos
- Associated branding
- Associated visual elements

Additional trademarks shall be developed, acquired, registered, or used in the future.

153.2 Trademark Protections

Trademarks are protected by applicable intellectual property laws.

Unauthorized use of trademarks shall create confusion, dilute brand value, misrepresent affiliation, or otherwise infringe intellectual property rights.

Users shall not:

- Copy trademarks
- Alter trademarks
- Misrepresent ownership
- Remove trademark notices
- Create confusingly similar branding
- Use trademarks in a misleading manner

153.3 Limited Reference Rights

Customers, partners, and authorized users shall reference Cognera Health trademarks solely as permitted under applicable agreements, policies, branding guidelines, or written authorization.

All goodwill associated with the trademarks shall remain the property of Cognera Health.

154. COPYRIGHTS

154.1 Copyright Ownership

Unless otherwise stated, all platform content is protected by copyright law.

Protected materials shall include:

- Software
- Interfaces
- Documentation
- Designs
- Reports
- Graphics
- Images
- Workflows
- Databases
- Content
- Training materials
- User guides
- Architecture diagrams
- Technical specifications

Copyright protection applies regardless of format.

154.2 Copyright Restrictions

Except as expressly authorized:

Users shall not:

- Copy content
- Reproduce content
- Republish content

- Modify content
- Distribute content
- Commercialize content
- Create derivative works
- Remove copyright notices

Unauthorized use shall violate intellectual property laws.

155. PROPRIETARY TECHNOLOGY

155.1 Technology Ownership

Cognera Health retains ownership of all proprietary technology developed, licensed, acquired, maintained, enhanced, operated, or controlled by the organization.

Proprietary technology shall include:

- Platforms
- Software
- Applications
- APIs
- Workflows
- Data models
- Architectures
- Automation frameworks
- AI technologies
- Integration frameworks
- Security systems
- Analytics engines

Ownership remains with Cognera Health regardless of customer use.

155.2 Trade Secrets

Certain technology components shall constitute trade secrets.

Trade secret protections shall apply to:

- Technical processes
- Business processes

- Architectures
- Models
- Algorithms
- Methodologies
- Designs
- Workflows
- Internal procedures

Trade secrets shall not be disclosed without authorization.

156. AI MODELS

156.1 Ownership

AI models developed, licensed, customized, configured, enhanced, operated, or maintained by Cognera Health remain the property of Cognera Health or its licensors.

Ownership includes:

- Model architecture
- Model design
- Model configuration
- Fine-tuning methods
- Evaluation frameworks
- Validation frameworks
- Governance frameworks
- Monitoring frameworks

Use of AI functionality does not transfer ownership rights.

156.2 AI Improvements

Any enhancements, modifications, optimizations, tuning activities, governance activities, monitoring activities, validation activities, or performance improvements relating to AI systems remain the property of Cognera Health unless otherwise agreed in writing.

157. ALGORITHMS

157.1 Ownership

Algorithms utilized within the platform remain proprietary.

Algorithms shall support:

- Analytics
- Classification
- Recommendation generation
- Workflow automation
- Risk visibility
- Trend analysis
- Reporting
- Security functions
- Operational intelligence

Algorithmic methodologies represent proprietary intellectual property.

157.2 Restrictions

Users shall not attempt to:

- Reverse engineer algorithms
- Extract algorithms
- Replicate algorithms
- Analyze algorithms for competitive purposes
- Decompile algorithms
- Circumvent protections

Unauthorized activities shall violate intellectual property rights.

158. SOURCE CODE

158.1 Ownership

All source code associated with Cognera Health products remains proprietary.

Source code ownership includes:

- Application code
- Backend code
- APIs
- Integrations
- Automation code
- Security code
- Infrastructure code
- AI-related code

Customers receive access to services—not ownership of source code.

158.2 Restrictions

Users shall not:

- Access source code
- Decompile software
- Reverse engineer software
- Derive source code
- Modify software
- Create derivative versions

unless expressly authorized in writing.

159. DOCUMENTATION

159.1 Ownership

Documentation remains the property of Cognera Health.

Documentation shall include:

- User guides
- Training materials
- Technical specifications
- Security documentation
- Compliance documentation
- Product descriptions
- Governance documentation

- Operational documentation

Documentation is protected by intellectual property laws.

159.2 Permitted Use

Authorized users shall use documentation solely for purposes related to authorized use of services.

Documentation shall not be redistributed without authorization.

160. PLATFORM RIGHTS

160.1 Ownership of Platform

Cognera Health retains all rights, title, and interest in and to the platform.

Platform ownership includes:

- Interfaces
- Features
- Functionality
- Design
- Workflows
- Databases
- Services
- Configurations
- Analytics
- Reporting systems
- AI systems
- Security systems

Customer access does not create ownership rights.

160.2 License Rights

Customers receive limited, revocable, non-exclusive, non-transferable rights to access and use services in accordance with applicable agreements.

All rights not expressly granted are reserved.

161. CUSTOMER DATA OWNERSHIP

161.1 Customer Ownership

Except as otherwise required by law or contract, customers retain ownership of customer-provided information.

Examples include:

- Clinical records
- Assessments
- Notes
- Organizational records
- User-generated information
- Uploaded information

Ownership of customer information remains distinct from ownership of the platform.

161.2 Platform Ownership

Although customers shall own customer information, Cognera Health retains ownership of:

- Software
- Infrastructure
- Models
- Interfaces
- Analytics engines
- Workflows
- Security controls
- Platform technologies

Ownership of data does not create ownership of technology.

162. FEEDBACK RIGHTS

162.1 Feedback

Users shall voluntarily provide:

- Suggestions
- Ideas
- Enhancements

- Recommendations
- Feedback
- Feature requests
- Comments

Feedback is appreciated and shall contribute to platform improvements.

162.2 License to Feedback

Unless prohibited by law, users grant Cognera Health a perpetual, irrevocable, worldwide, royalty-free right to use, modify, incorporate, commercialize, and otherwise utilize feedback without compensation.

Feedback shall be used to improve products and services.

163. OPEN SOURCE COMPONENTS

163.1 Third-Party Software

Certain services shall include open source software components.

Open source components remain subject to their applicable licenses.

163.2 License Compliance

Cognera Health seeks to comply with applicable open source licensing requirements.

Open source licenses apply only to applicable components and do not affect ownership of proprietary platform components.

164. RESTRICTIONS

Users shall not:

- Reverse engineer services
- Decompile services
- Replicate services
- Extract models
- Copy workflows

- Create competing products using platform assets
- Remove proprietary notices
- Misappropriate intellectual property
- Circumvent protections
- Use services beyond authorized purposes

Unauthorized activities shall result in suspension, termination, legal action, or other remedies.

165. RESERVATION OF RIGHTS

Except for rights expressly granted through written agreements, Cognera Health reserves all rights, title, interests, protections, remedies, and intellectual property rights.

No implied license shall be created through platform use.

No ownership rights shall transfer absent an explicit written agreement.

166. ENFORCEMENT

166.1 Protection of Rights

Cognera Health reserves the right to protect and enforce its intellectual property rights to the fullest extent permitted by law.

Enforcement activities shall include:

- Investigations
- Notices
- Takedown requests
- Contractual remedies
- Injunctive relief
- Legal proceedings
- Regulatory actions
- Other lawful remedies

166.2 Preservation of Remedies

Failure to enforce a provision at a particular time shall not constitute a waiver of rights.

Cognera Health reserves all legal, equitable, contractual, and statutory remedies available under applicable law.

Intellectual property rights remain protected regardless of whether enforcement actions are immediately pursued.

PART XV – ACCEPTABLE USE POLICY

167. PURPOSE

167.1 Purpose of Policy

The Acceptable Use Policy ("AUP") establishes requirements governing the appropriate, lawful, ethical, secure, and responsible use of Cognera Health™ products, services, technologies, applications, platforms, artificial intelligence systems, websites, APIs, integrations, communication systems, reporting systems, analytics systems, operational intelligence systems, enterprise intelligence systems, and related services.

The purpose of this Policy is to:

- Protect users
- Protect customers
- Protect healthcare organizations
- Protect platform integrity
- Protect information
- Protect privacy
- Protect security
- Protect operational resilience
- Protect intellectual property
- Support regulatory compliance
- Support responsible AI use

The Acceptable Use Policy applies to all users, customers, administrators, healthcare professionals, care teams, organizations, vendors, contractors, partners, and other authorized users.

167.2 User Responsibilities

Users are expected to:

- Use services responsibly
- Follow applicable laws
- Follow applicable regulations
- Follow professional obligations
- Follow organizational policies
- Respect privacy rights
- Respect security requirements
- Respect intellectual property rights
- Protect confidential information
- Protect customer information
- Protect healthcare information

Use of the platform constitutes agreement to comply with this Policy.

168. PROHIBITED ACTIVITIES

168.1 General Prohibition

Users shall not engage in activities that:

- Violate laws
- Violate regulations
- Violate contractual obligations
- Violate professional obligations
- Violate organizational policies
- Violate privacy rights
- Violate security requirements
- Harm others
- Disrupt services
- Undermine platform integrity

Activities not specifically listed shall still be prohibited if they present unacceptable risks.

168.2 Illegal Activities

Users shall not use the platform to:

- Commit crimes
- Facilitate crimes
- Conceal crimes
- Support unlawful activity
- Evade legal obligations
- Violate sanctions
- Violate export controls
- Engage in fraud
- Engage in deception
- Engage in identity theft
- Engage in unauthorized surveillance

The platform shall not be used for unlawful purposes under any circumstances.

168.3 Harmful Activities

Users shall not engage in activities intended to:

- Harm individuals
- Harm organizations
- Harass individuals
- Threaten individuals
- Intimidate individuals
- Facilitate violence
- Facilitate abuse
- Facilitate discrimination
- Facilitate unlawful conduct

Cognera Health reserves the right to investigate and respond to harmful conduct.

169. SECURITY VIOLATIONS

169.1 Unauthorized Access

Users shall not attempt to gain unauthorized access to:

- Systems
- Applications
- APIs

- Databases
- Infrastructure
- Networks
- Accounts
- Services

Unauthorized access includes attempts to exceed assigned permissions.

169.2 Credential Misuse

Users shall not:

- Share credentials
- Sell credentials
- Transfer credentials
- Steal credentials
- Misuse credentials
- Circumvent authentication
- Circumvent authorization

Credentials must be protected at all times.

169.3 Security Testing Without Authorization

Users shall not perform unauthorized:

- Penetration testing
- Vulnerability scanning
- Security assessments
- Exploitation activities
- Red team activities
- Security research

Security testing must be expressly authorized through approved processes.

169.4 Malware and Malicious Code

Users shall not introduce:

- Malware
- Ransomware
- Viruses
- Trojans
- Spyware
- Backdoors
- Malicious scripts
- Harmful payloads

Any attempt to compromise platform security is strictly prohibited.

170. DATA MISUSE

170.1 Unauthorized Data Access

Users shall not access information that they are not authorized to access.

Authorization requirements apply regardless of technical capability.

Possessing the ability to access information does not create authorization to access information.

170.2 Unauthorized Disclosure

Users shall not disclose:

- PHI
- ePHI
- Personal Information
- Consumer Health Data
- Confidential Information
- Proprietary Information
- Security Information

except as authorized.

Unauthorized disclosure shall result in disciplinary action, contractual remedies, regulatory consequences, or legal action.

170.3 Data Extraction

Users shall not:

- Bulk export information
- Copy information
- Transfer information
- Download information
- Extract information

except as expressly authorized.

Data extraction activities shall be monitored and restricted.

171. AI MISUSE

171.1 Responsible AI Use

AI-enabled functionality must be used responsibly.

Users shall not intentionally misuse AI systems.

AI tools are intended to support legitimate operational, administrative, healthcare, wellness, documentation, communication, and organizational purposes.

171.2 Prohibited AI Activities

Users shall not use AI functionality to:

- Generate unlawful content
- Generate fraudulent content
- Impersonate individuals
- Mislead users
- Manipulate records
- Create false documentation
- Create deceptive content
- Circumvent safeguards
- Abuse AI systems
- Generate harmful content

AI-generated outputs remain subject to human review requirements.

171.3 AI Safety Circumvention

Users shall not attempt to:

- Disable AI safeguards
- Bypass AI controls
- Manipulate AI restrictions
- Override safety controls
- Exploit AI systems

Attempts to circumvent AI controls shall result in immediate suspension.

172. REVERSE ENGINEERING

172.1 Prohibited Activities

Except where prohibited by law, users shall not:

- Reverse engineer
- Decompile
- Disassemble
- Replicate
- Reconstruct
- Analyze source code
- Extract proprietary logic
- Derive trade secrets

These restrictions apply to:

- Applications
- APIs
- Models
- Algorithms
- Integrations
- Infrastructure
- Workflows

172.2 Competitive Use Restrictions

Users shall not use platform access to:

• Build competing services

• Replicate functionality

• Copy workflows

• Replicate models

• Replicate interfaces

• Replicate analytics

Platform access shall not be used for competitive intelligence activities.

173. AUTOMATED SCRAPING

173.1 Prohibited Scraping Activities

Users shall not engage in unauthorized:

- Web scraping
- Data harvesting
- Data extraction
- Content scraping
- Automated collection
- Crawling
- Indexing
- Bot activity

Scraping shall negatively impact privacy, security, performance, and intellectual property protections.

173.2 Automated Access Restrictions

Automated access requires authorization.

Unauthorized bots, crawlers, scripts, agents, and automation systems are prohibited.

Cognera Health shall implement technical controls to detect and prevent unauthorized automation.

174. ABUSE PREVENTION

174.1 Platform Protection

Cognera Health maintains controls intended to protect users, organizations, information, and services from abuse.

Abusive activities shall include:

- Harassment
- Threats
- Fraud
- Deception
- Security attacks
- Resource abuse
- System manipulation
- AI misuse
- Privacy violations

Abuse prevention supports platform safety and operational integrity.

174.2 Monitoring Activities

Cognera Health shall monitor activities for indicators of abuse, misuse, fraud, security threats, policy violations, operational disruptions, or unauthorized conduct.

Monitoring activities are conducted consistent with applicable legal, contractual, privacy, and security requirements.

175. USER CONDUCT STANDARDS

175.1 Professional Conduct

Users are expected to behave in a professional, lawful, ethical, and respectful manner.

Professional conduct supports:

- Trust
- Safety
- Collaboration
- Compliance

- Operational effectiveness

Users remain responsible for their actions while using the platform.

175.2 Respect for Others

Users should not:

- Harass others
- Threaten others
- Intimidate others
- Abuse others
- Discriminate against others
- Create hostile environments

The platform should be used in a manner consistent with organizational values and professional standards.

176. PLATFORM INTEGRITY PROTECTIONS

176.1 Service Integrity

Users shall not intentionally interfere with:

- Platform operations
- Service availability
- Security controls
- Monitoring systems
- Reporting systems
- Analytics systems
- Infrastructure

Activities that degrade reliability, stability, security, or availability are prohibited.

176.2 Resource Abuse

Users shall not consume excessive resources in a manner that negatively affects:

- Performance
- Availability

- Reliability
- Customer experience

Resource abuse shall result in restrictions or suspension.

177. ENFORCEMENT ACTIONS

177.1 Enforcement Authority

Cognera Health reserves the right to investigate suspected violations of this Policy.

Investigations shall involve:

- Security reviews
- Compliance reviews
- Privacy reviews
- Operational reviews
- Legal reviews

Investigations shall be conducted with or without advance notice.

177.2 Corrective Actions

Where violations are identified, Cognera Health shall implement:

- Warnings
- Restrictions
- Monitoring
- Remediation requirements
- Access limitations
- Suspension
- Termination
- Legal action

The response shall vary depending upon severity and risk.

178. SUSPENSION CRITERIA

178.1 Immediate Suspension

Cognera Health shall immediately suspend access where activities present:

- Security risks
- Privacy risks
- Compliance risks
- Safety risks
- Operational risks
- Legal risks

Immediate action shall be necessary to protect users, customers, organizations, or services.

178.2 Temporary or Permanent Suspension

Suspensions shall be:

- Temporary
- Conditional
- Indefinite
- Permanent

Suspension decisions shall consider:

- Severity
- Intent
- Impact
- Risk
- Prior conduct

179. REPORTING MISUSE

179.1 Reporting Channels

Users are encouraged to report suspected:

- Security violations
- Privacy violations
- Policy violations
- Fraud
- Abuse
- AI misuse

- Harassment
- Unauthorized access

Reports shall be submitted through:

- security@cogneraheath.ai
- compliance@cogneraheath.ai
- privacy@cogneraheath.ai
- support@cogneraheath.ai

or other designated reporting channels.

179.2 Investigation and Response

Reported concerns shall be reviewed, investigated, documented, escalated, and addressed according to applicable governance, compliance, privacy, security, legal, and operational procedures.

Cognera Health reserves the right to take appropriate action to protect users, customers, organizations, information, services, and platform integrity.

179.3 Non-Retaliation

Cognera Health supports good-faith reporting of concerns.

Individuals who report concerns in good faith should not be subject to retaliation solely for raising legitimate concerns regarding security, privacy, compliance, accessibility, safety, misuse, fraud, or other policy violations.

PART XVI – REGULATORY COMPLIANCE & GOVERNANCE ALIGNMENT

180. REGULATORY COMPLIANCE OVERVIEW

180.1 Purpose

Cognera Health™ maintains governance, privacy, security, accessibility, risk management, operational resilience, artificial intelligence governance, and compliance programs intended to support applicable legal, regulatory, contractual, and industry requirements.

The purpose of this section is to provide transparency regarding regulatory frameworks, standards, guidance, and governance practices that shall inform the design, operation, maintenance, monitoring, and continuous improvement of Cognera Health products and services.

References to laws, regulations, standards, frameworks, controls, certifications, guidance documents, industry practices, and governance methodologies are intended to describe alignment, support, consideration, implementation, or incorporation of controls informed by such requirements.

References should not be interpreted as representations of certification, accreditation, approval, endorsement, legal compliance, or regulatory approval unless expressly stated.

180.2 Compliance Philosophy

Cognera Health recognizes that healthcare technology operates within a highly regulated environment.

Accordingly, compliance activities are intended to support:

- Privacy protection
- Information security
- Patient protection
- Consumer protection
- Responsible AI
- Accessibility
- Operational resilience
- Governance accountability
- Risk management

- Continuous improvement

Compliance programs are intended to operate alongside organizational governance, security, privacy, accessibility, quality, legal, and operational programs.

181. HIPAA ALIGNMENT

181.1 HIPAA Overview

Where applicable, Cognera Health shall support compliance activities associated with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

HIPAA establishes requirements relating to:

- Privacy
- Security
- Administrative safeguards
- Technical safeguards
- Physical safeguards
- Breach notification
- Individual rights
- Protected Health Information

HIPAA considerations shall apply where Cognera Health functions as a Business Associate.

181.2 HIPAA Privacy Rule Alignment

Governance activities shall support Privacy Rule requirements including:

- Use and disclosure controls
- Minimum necessary principles
- Workforce training
- Access management
- Individual rights support
- Documentation requirements
- Administrative controls

Privacy controls are intended to support responsible handling of Protected Health Information.

181.3 HIPAA Security Rule Alignment

Security controls shall support requirements associated with:

- Risk management
- Workforce security
- Access controls
- Audit controls
- Integrity controls
- Authentication
- Transmission security
- Security incident response

Security programs are intended to support protection of ePHI.

181.4 HIPAA Breach Notification Alignment

Incident response activities shall support breach assessment and notification obligations where applicable.

Notification obligations shall depend upon:

- Incident characteristics
- Regulatory requirements
- Contractual requirements
- Legal obligations

182. HITECH ALIGNMENT

182.1 HITECH Overview

Where applicable, Cognera Health shall support requirements associated with the Health Information Technology for Economic and Clinical Health Act ("HITECH").

HITECH considerations shall include:

- Breach notification
- Security enhancement
- Enforcement requirements
- Business Associate obligations

- Electronic health information protections

HITECH considerations are incorporated into broader governance, privacy, and security activities.

182.2 Security Enhancement Objectives

Security programs shall support HITECH objectives through:

- Risk assessments
- Monitoring
- Security controls
- Encryption
- Incident response
- Workforce awareness
- Governance oversight

HITECH activities complement HIPAA-related obligations.

183. GDPR ALIGNMENT

183.1 GDPR Overview

Where applicable, Cognera Health shall support compliance activities associated with the General Data Protection Regulation ("GDPR").

GDPR considerations shall include:

- Lawful processing
- Transparency
- Accountability
- Data subject rights
- Privacy by design
- Security
- Data minimization
- Purpose limitation
- Cross-border transfers
- Governance requirements

183.2 GDPR Principles

Privacy programs shall support principles including:

- Lawfulness
- Fairness
- Transparency
- Accuracy
- Data minimization
- Storage limitation
- Integrity
- Confidentiality
- Accountability

These principles shall inform privacy governance activities.

183.3 Data Subject Rights

Where applicable, GDPR-related processes shall support:

- Access requests
- Rectification requests
- Erasure requests
- Restriction requests
- Objection requests
- Portability requests
- Consent withdrawal

Rights remain subject to applicable legal limitations and exceptions.

184. UK GDPR ALIGNMENT

184.1 UK GDPR Overview

Where applicable, Cognera Health shall support compliance activities associated with the United Kingdom General Data Protection Regulation.

UK GDPR considerations shall include:

- Privacy governance

- Data rights
- International transfers
- Security
- Accountability
- Transparency

UK GDPR activities shall be integrated with broader privacy governance programs.

185. CCPA ALIGNMENT

185.1 California Consumer Privacy Act

Where applicable, Cognera Health shall support requirements associated with the California Consumer Privacy Act ("CCPA").

CCPA considerations shall include:

- Notice requirements
- Consumer rights
- Data access rights
- Data deletion rights
- Non-discrimination requirements
- Governance obligations

Consumer rights processes shall support lawful handling of applicable requests.

186. CPRA ALIGNMENT

186.1 California Privacy Rights Act

The California Privacy Rights Act ("CPRA") expanded California privacy requirements.

CPRA-related governance activities shall include:

- Sensitive information protections
- Risk assessments
- Consumer rights
- Transparency activities
- Privacy governance enhancements

Privacy programs shall incorporate CPRA-informed controls where applicable.

187. CONSUMER HEALTH PRIVACY LAWS

187.1 State Consumer Health Privacy Requirements

Consumer health privacy laws continue to evolve.

Examples shall include:

- Washington My Health My Data Act
- Nevada consumer health requirements
- Connecticut requirements
- Other emerging state laws

Cognera Health monitors developments that shall affect processing of consumer health data.

187.2 Consumer Health Data Governance

Governance activities shall include:

- Consent management
- Privacy notices
- Data rights
- Data minimization
- Retention controls
- Sharing controls

Consumer health data protections shall be incorporated into broader privacy programs.

188. TELEHEALTH LAWS

188.1 Telehealth Regulatory Considerations

Telehealth-related functionality shall be affected by federal, state, provincial, local, professional, licensing, and organizational requirements.

Telehealth obligations shall vary significantly across jurisdictions.

Organizations remain responsible for compliance with applicable telehealth requirements.

188.2 Provider Responsibilities

Healthcare providers remain responsible for:

- Licensure
- Scope of practice
- Clinical obligations
- Consent requirements
- Documentation requirements
- Emergency procedures
- Patient communications

Technology functionality does not replace provider obligations.

189. NIST AI RMF ALIGNMENT

189.1 Overview

Cognera Health shall consider concepts reflected in the NIST Artificial Intelligence Risk Management Framework (AI RMF).

AI RMF concepts shall inform:

- Governance
- Mapping
- Measurement
- Management
- Risk assessments
- Monitoring
- Continuous improvement

189.2 Responsible AI Alignment

AI governance activities shall incorporate AI RMF principles relating to:

- Accountability
- Transparency
- Safety
- Reliability
- Privacy

- Security
- Fairness
- Human oversight

190. NIST CYBERSECURITY FRAMEWORK (CSF)

190.1 Overview

Cognera Health shall consider concepts reflected in the NIST Cybersecurity Framework.

Framework functions shall include:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

These concepts shall inform security governance activities.

190.2 Security Program Alignment

Security programs shall utilize CSF concepts for:

- Risk management
- Security assessments
- Incident response
- Monitoring
- Recovery planning
- Governance activities

191. NIST SP 800-53 ALIGNMENT

191.1 Control Framework

Cognera Health shall consider security and privacy control concepts reflected in NIST SP 800-53.

Control families shall include:

- Access Control
- Audit and Accountability
- Incident Response
- Risk Assessment
- Configuration Management
- Contingency Planning
- System Integrity
- Security Assessment

Controls shall inform security program design.

192. ISO 27001 ALIGNMENT

192.1 Information Security Management

Cognera Health shall utilize concepts reflected in ISO/IEC 27001.

ISO 27001 concepts shall inform:

- Governance
- Risk management
- Security controls
- Policies
- Procedures
- Continuous improvement

Security programs shall align with information security management principles.

193. ISO 27701 ALIGNMENT

193.1 Privacy Information Management

Cognera Health shall consider concepts reflected in ISO/IEC 27701.

Privacy governance activities shall incorporate concepts including:

- Privacy controls
- Privacy governance
- Accountability

- Data protection
- Data subject rights
- Documentation

Privacy management activities shall be informed by these principles.

194. HITRUST CSF ALIGNMENT

194.1 Healthcare Security Framework

Cognera Health shall consider concepts reflected in the HITRUST Common Security Framework (CSF).

HITRUST concepts shall support:

- Healthcare security
- Privacy governance
- Risk management
- Compliance activities
- Control implementation

HITRUST-informed controls shall be integrated into broader governance activities.

195. SOC 2 ALIGNMENT

195.1 Trust Services Criteria

Cognera Health shall consider concepts reflected in the AICPA Trust Services Criteria associated with SOC 2.

Trust Services Criteria shall include:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

These concepts shall inform governance and operational activities.

196. FUTURE REGULATORY MONITORING

196.1 Evolving Regulatory Environment

Healthcare, privacy, cybersecurity, accessibility, artificial intelligence, consumer protection, telehealth, and operational regulations continue to evolve globally.

Cognera Health maintains monitoring activities intended to identify emerging obligations and regulatory developments.

196.2 Future AI Regulations

Future regulations shall address:

- Artificial Intelligence
- Algorithmic accountability
- Transparency
- Human oversight
- Automated decision-making
- AI safety
- AI governance
- AI documentation
- AI auditing

Cognera Health shall modify policies, procedures, controls, technologies, governance activities, and operational practices to address future requirements.

196.3 Continuous Compliance Improvement

Regulatory monitoring supports:

- Governance enhancements
- Policy updates
- Control improvements
- Operational improvements
- Documentation updates
- Risk management activities
- Training activities

Continuous improvement remains a foundational component of Cognera Health's compliance philosophy.

PART XVII – LEGAL TERMS & GENERAL PROVISIONS

197. DISCLAIMER OF WARRANTIES

197.1 General Disclaimer

To the fullest extent permitted by applicable law, Cognera Health™, HealScript™, HealConnect™, CogneraAI™, websites, mobile applications, APIs, integrations, documentation, analytics services, reporting services, operational intelligence services, enterprise intelligence services, artificial intelligence services, communication services, telehealth-related functionality, and all related services are provided on an:

"AS IS"

"AS AVAILABLE"

"WITH ALL FAULTS"

basis.

Cognera Health makes no representations, warranties, guarantees, commitments, promises, or assurances regarding:

- Availability
- Accuracy
- Completeness
- Reliability
- Performance
- Security
- Accessibility
- Functionality
- Regulatory suitability
- Clinical suitability
- Business suitability
- Fitness for a particular purpose

197.2 No Medical Warranty

Cognera Health does not warrant that:

- Information is clinically appropriate
- AI outputs are clinically accurate
- Recommendations are medically appropriate
- Documentation is accurate
- Assessments are complete
- Analytics are correct
- Predictions are accurate
- Outcomes will improve
- Risks will be identified
- Clinical decisions will be supported appropriately

Clinical responsibility remains with licensed healthcare professionals.

197.3 No Availability Warranty

Cognera Health does not guarantee:

- Continuous availability
- Uninterrupted service
- Error-free operation
- Compatibility with all systems
- Availability of all features
- Availability of all integrations

Services shall experience interruptions caused by:

- Maintenance
- Upgrades
- Security events
- Infrastructure failures
- Third-party disruptions
- Internet outages
- Force majeure events

197.4 AI Disclaimer

Artificial intelligence systems may:

- Hallucinate
- Generate inaccurate information
- Generate incomplete information
- Produce biased outputs
- Produce inconsistent outputs
- Produce outdated outputs

AI outputs must always be independently reviewed.

No warranty is made regarding AI-generated content.

198. LIMITATION OF LIABILITY

198.1 Limitation

To the fullest extent permitted by law, Cognera Health shall not be liable for any:

- Indirect damages
- Incidental damages
- Special damages
- Consequential damages
- Exemplary damages
- Punitive damages
- Lost profits
- Lost revenue
- Lost opportunities
- Lost savings
- Lost business
- Loss of goodwill
- Data loss
- Service interruption
- Business interruption

arising from or related to use of the Services.

198.2 AI-Related Liability

Cognera Health shall not be liable for decisions made using AI-generated outputs.

Users acknowledge that:

- AI outputs require validation
- AI outputs require review
- AI outputs shall contain errors
- Human oversight is required

Responsibility for decisions remains with authorized users.

198.3 Healthcare Decisions

Cognera Health shall not be liable for:

- Clinical decisions
- Treatment decisions
- Prescribing decisions
- Diagnostic decisions
- Risk assessments
- Care coordination decisions
- Crisis response decisions
- Emergency response decisions

Healthcare professionals remain solely responsible for healthcare decisions.

198.4 Maximum Liability

To the fullest extent permitted by law, aggregate liability arising from use of the Services shall not exceed amounts paid by the applicable customer during the twelve (12) months immediately preceding the event giving rise to the claim.

Where no fees have been paid, liability shall be limited to the maximum extent permitted by law.

199. INDEMNIFICATION

199.1 User Indemnification

Users agree to defend, indemnify, and hold harmless Cognera Health and its:

- Officers
- Directors
- Employees
- Contractors
- Affiliates
- Successors
- Agents

from claims arising out of:

- Violations of this Framework
- Violations of law
- User misconduct
- Unauthorized access
- Unauthorized disclosures
- Data misuse
- Security incidents caused by users
- Professional negligence
- Clinical negligence
- Regulatory violations

199.2 Customer Indemnification

Organizations utilizing the platform agree to indemnify Cognera Health against claims resulting from:

- Healthcare services delivered by the organization
- Clinical decisions
- Provider conduct
- Professional malpractice
- Regulatory violations
- Misuse of platform services
- Unauthorized processing of information

199.3 Survival

Indemnification obligations survive termination of services and expiration of agreements.

200. FORCE MAJEURE

200.1 Force Majeure Events

Cognera Health shall not be liable for delays, interruptions, failures, disruptions, or inability to perform caused by events beyond reasonable control.

Examples include:

- Natural disasters
- Floods
- Hurricanes
- Earthquakes
- Fires
- Pandemics
- Epidemics
- War
- Terrorism
- Civil unrest
- Labor disputes
- Government actions
- Utility failures
- Internet outages
- Cloud provider failures
- Cyberattacks
- Infrastructure failures
- Supply chain disruptions

200.2 Continuity Efforts

Cognera Health will make commercially reasonable efforts to restore services following force majeure events.

However, no guarantee can be made regarding recovery timelines.

201. SUSPENSION RIGHTS

201.1 Right to Suspend

Cognera Health shall suspend access immediately where necessary to protect:

- Security
- Privacy
- Compliance
- Availability
- Customers
- Users
- Infrastructure
- Information

Suspension shall occur with or without prior notice where circumstances require immediate action.

201.2 Suspension Triggers

Examples include:

- Security threats
- Policy violations
- Regulatory concerns
- Fraud
- Abuse
- Unauthorized access
- Malware activity
- Operational risks
- Legal obligations

202. TERMINATION RIGHTS

202.1 Termination by User

Users shall discontinue use of services at any time, subject to applicable contractual obligations.

202.2 Termination by Cognera Health

Cognera Health shall terminate access where:

- This Framework is violated
- Security risks arise
- Fraud occurs
- Misuse occurs
- Legal obligations require termination
- Services are discontinued

202.3 Effect of Termination

Upon termination:

- Access rights cease
- Licenses terminate
- User access shall be removed
- Information shall be retained according to retention obligations
- Certain obligations survive termination

203. EXPORT CONTROLS

203.1 Compliance

Users agree to comply with all applicable export control laws and regulations.

Services shall not be used in violation of export restrictions.

203.2 Restricted Activities

Users shall not export, transfer, disclose, or provide access to services where prohibited by applicable law.

204. SANCTIONS COMPLIANCE

204.1 Compliance Requirements

Users shall not utilize services in violation of applicable sanctions laws or restrictions.

204.2 Restricted Parties

Services shall not be used by:

- Restricted parties
- Sanctioned entities
- Prohibited organizations
- Persons prohibited under applicable law

Cognera Health reserves the right to restrict access where required.

205. ASSIGNMENT

205.1 User Assignment Restrictions

Users shall not assign rights or obligations under this Framework without prior written consent.

205.2 Cognera Health Assignment Rights

Cognera Health shall assign rights, obligations, agreements, assets, or services in connection with:

- Reorganizations
- Acquisitions
- Mergers
- Corporate restructurings
- Asset transfers

206. GOVERNING LAW

206.1 Governing Jurisdiction

This Framework shall be governed by the laws of the State of Delaware, without regard to conflict of law principles.

206.2 Regulatory Requirements

Nothing in this Framework shall limit rights or obligations imposed by applicable law.

207. DISPUTE RESOLUTION

207.1 Informal Resolution

Parties agree to attempt good-faith resolution of disputes prior to initiating formal proceedings.

207.2 Arbitration

Where permitted by law, disputes shall be resolved through binding arbitration.

Arbitration procedures shall be conducted according to applicable arbitration rules.

207.3 Venue

Where arbitration does not apply, disputes shall be resolved in courts located in Delaware unless otherwise required by law.

208. CLASS ACTION WAIVER

208.1 Individual Proceedings

To the fullest extent permitted by law, disputes shall be brought on an individual basis.

Users waive participation in:

- Class actions
- Collective actions

- Representative actions
- Mass proceedings

except where prohibited by law.

208.2 Severability

If the class action waiver is determined unenforceable, remaining provisions shall remain in effect to the fullest extent permitted by law.

209. SEVERABILITY

209.1 Partial Invalidity

If any provision of this Framework is determined to be invalid, unlawful, or unenforceable, remaining provisions shall remain in full force and effect.

209.2 Modification

Invalid provisions shall be modified to the minimum extent necessary to make them enforceable while preserving original intent.

210. ENTIRE AGREEMENT

210.1 Entire Understanding

This Framework, together with referenced policies and applicable agreements, constitutes the entire understanding regarding the subject matter addressed herein.

210.2 Order of Precedence

Where applicable:

1. Executed Enterprise Agreements
2. Business Associate Agreements
3. Data Processing Addenda
4. Service Level Agreements
5. Security Exhibits

6. Responsible AI Addenda
7. This Framework
8. Public Website Content

unless otherwise stated.

211. CHANGES TO FRAMEWORK

211.1 Right to Update

Cognera Health shall update this Framework periodically.

Updates shall occur due to:

- Regulatory developments
- Technology changes
- Security improvements
- Privacy improvements
- Accessibility improvements
- Governance enhancements
- Operational changes

211.2 Notice of Changes

Updated versions shall be published through:

- Websites
- Trust Center
- Customer communications
- Platform notifications

Continued use following updates shall constitute acceptance where permitted by law.

212. CONTACT INFORMATION

212.1 General Contact

Cognera Health, Inc.

- Website:
  - www.cogneraheath.ai
- General Inquiries:
  - info@cogneraheath.ai

212.2 Privacy

privacy@cogneraheath.ai

- For:
  - Privacy requests
  - Data rights requests
  - Privacy concerns
  - Privacy complaints

212.3 Security

security@cogneraheath.ai

- For:
  - Security concerns
  - Vulnerability disclosures
  - Security incidents
  - Security questions

212.4 Compliance

compliance@cogneraheath.ai

- For:
  - Compliance inquiries
  - Regulatory matters
  - Governance inquiries
  - Audit inquiries

212.5 Accessibility

accessibility@cogneraheath.ai

For:

- Accessibility concerns
- Accommodation requests
- Accessibility feedback

212.6 AI Governance

ai-governance@cogneraheath.ai

For:

- Responsible AI inquiries
- AI governance concerns
- AI transparency requests
- AI risk concerns

212.7 Legal

legal@cogneraheath.ai

For:

- Legal notices
- Contractual matters
- Intellectual property matters
- Dispute-related communications

213. CONCLUSION

This Cognera Health™ Platform Governance, Terms, Security, Privacy, Accessibility & Responsible AI Framework establishes the foundational governance, privacy, security, accessibility, compliance, responsible artificial intelligence, operational resilience, intellectual property, acceptable use, and legal principles governing the Cognera Health ecosystem.

The Framework is intended to support transparency, accountability, trust, safety, security, privacy, accessibility, regulatory alignment, and responsible innovation while enabling organizations, healthcare professionals, care teams, and individuals to utilize technology in support of continuous, connected, and coordinated care.

PART XVIII – APPENDICES & CONTROL MAPPING MATRIX

APPENDIX A – GOVERNANCE FRAMEWORK HIERARCHY

Governance Document Hierarchy

Level 1 – Governance Framework

Cognera Health™ Platform Governance, Terms, Security, Privacy, Accessibility & Responsible AI Framework

Level 2 – Governance Programs

- Privacy Program
- Security Program
- Responsible AI Program
- Accessibility Program
- Compliance Program
- Risk Management Program
- Business Continuity Program

Level 3 – Supporting Policies

- Privacy Policy
- Data Retention Policy
- Data Deletion Policy
- Acceptable Use Policy
- Vulnerability Disclosure Policy
- AI Governance Policy
- Incident Response Policy
- Accessibility Policy

Level 4 – Operational Standards

- Procedures
- Work Instructions
- Technical Standards
- Control Standards

Level 5 – Operational Records

- Logs
- Reports

- Assessments
- Reviews
- Audit Evidence

APPENDIX B – REGULATORY CONTROL MAPPING METHODOLOGY

The mappings contained in this Appendix are intended to identify regulatory, security, privacy, AI governance, accessibility, and operational frameworks that informed development of the Cognera Health governance program.

References indicate:

- Alignment
- Support
- Consideration
- Implementation of related controls

References do not imply:

- Certification
- Accreditation
- Regulatory approval
- Legal determination

unless expressly stated.

APPENDIX C – SECTION TO REGULATORY CONTROL MATRIX

Framework Section	Subject Area	HIPAA	HITECH	GDPR	UK GDPR	CCPA/CPRA
Sections 1-7	Governance & Definitions	164.308(a)(1)	Administrative Safeguards	Articles 5,24	Articles 5,24	Governance Requirements
Sections 8-11	Products & Services	164.308	HITECH Security	Articles 25,32	Articles 25,32	Service Transparency
Sections 12-31	Healthcare & Emergency Disclaimers	Privacy Rule	HITECH	Articles 12-14	Articles 12-14	Consumer Notices

Framework Section	Subject Area	HIPAA	HITECH	GDPR	UK GDPR	CCPA/CPRA
Sections 32-54	AI Governance & Human Oversight	N/A	N/A	Articles 5,22	Articles 5,22	Automated Decision Controls
Sections 55-83	AI Risk Management	N/A	N/A	Articles 22,25,35	Articles 22,25,35	Risk Assessment Requirements
Sections 84-103	Privacy & Data Rights	Privacy Rule	HITECH	Articles 5-23	Articles 5-23	CCPA/CPRA Rights
Sections 104-127	Security Program	Security Rule	Security Rule	Article 32	Article 32	Reasonable Security
Sections 128-137	Vulnerability Disclosure	Security Rule	Security Rule	Article 32	Article 32	Security Controls
Sections 138-151	Accessibility	N/A	N/A	Article 25	Article 25	Consumer Access Rights
Sections 152-166	Intellectual Property	N/A	N/A	N/A	N/A	N/A
Sections 167-179	Acceptable Use	Security Rule	Security Rule	Article 32	Article 32	Security Obligations
Sections 180-196	Regulatory Alignment	All	All	All	All	All
Sections 197-212	Legal Terms	N/A	N/A	Articles 12-14	Articles 12-14	Consumer Notices

APPENDIX D – CONTINUOUS COMPLIANCE MONITORING MATRIX

Monitoring Activities

- Governance Reviews
- Privacy Reviews
- Security Reviews
- AI Reviews
- Accessibility Reviews
- Compliance Reviews
- Vendor Reviews
- Incident Reviews

- Risk Reviews

Review Frequencies

- Continuous
- Daily
- Weekly
- Monthly
- Quarterly
- Annually
- Event Driven

Corrective Action Process

1. Identify
2. Assess
3. Escalate
4. Remediate
5. Validate
6. Monitor
7. Close
8. Improve

This Appendix serves as the enterprise traceability layer connecting all governance, privacy, security, accessibility, AI governance, compliance, and operational controls to applicable regulatory, standards, and framework requirements.

APPENDIX E – SECTION-BY-CONTROL TRACEABILITY MATRIX

Important Mapping Notice

This traceability matrix is intended to support governance, procurement, audit readiness, compliance review, and control alignment activities. It is not a certification, legal opinion, regulatory determination, audit report, attestation, or guarantee of compliance.

Specific control applicability depends on Cognera Health's implemented controls, customer contracts, system architecture, processing activities, jurisdictional scope, risk profile, and operational maturity.

HITRUST CSF mappings should be finalized against the licensed HITRUST CSF version used by the organization.

E.1 TRACEABILITY MATRIX

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
1	Purpose	45 CFR §164.308(a)(1)(i)	Arts. 5, 24	Governance / Notice	PM-1, PM-9	A.5.1, A.5.2	Privacy governance	CC1, CC2	Governance / Risk Mgmt
2	Scope	45 CFR §164.308(a)(1)(ii)(A)	Arts. 5, 24, 25	Notice / Scope	PL-2, RA-3	A.5.9, A.5.31	PII scope	CC2, CC3	Risk Mgmt
3	Intended Audience	45 CFR §164.520	Arts. 12–14	Notice at Collection	PL-2, AC-1	A.5.10, A.5.31	Transparency	CC2	Privacy Governance
4	Relationship to Privacy Policy	45 CFR §164.520	Arts. 12–14	Privacy Notice	PL-2, PT-1	A.5.34	Privacy notices	CC2, P1	Privacy

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
5	Relationship to Trust Center	45 CFR §164.308(a)(1)	Arts. 5, 12, 24	Transparency	PM-1, PL-2	A.5.1, A.5.2	Transparency	CC1, CC2	Governance
6	Enterprise Agreements	45 CFR §164.314(a)	Arts. 28, 32	Service Provider Terms	SA-9, SR-3	A.5.19, A.5.20	Processor contracts	CC9	Third Party Risk
7	Definitions	45 CFR §160.103	Arts. 4, 5	Definitions / Scope	PL-2	A.5.31	Terminology	CC2	Governance
8	Cognera Platform Overview	45 CFR §164.308(a)(1)	Arts. 24, 25	Service Description	PL-2, SA-3	A.5.8, A.5.31	Privacy by design	CC2, CC3	Governance
9	HealScript™	45 CFR §164.308, §164.312	Arts. 25, 32	Reasonable Security	SA-8, AC-2	A.8.2, A.8.3	PII processing	CC6, CC7	Access / Security
10	HealConnect™	45 CFR §164.308, §164.312	Arts. 25, 32	Consumer Rights / Security	AC-2, IA-2	A.8.5, A.8.24	Data subject interaction	CC6, P1	Privacy / Security
11	CogneraAI™	HIPAA Security Rule where ePHI involved	Arts. 5, 22, 25, 32, 35	Automated Decisioning / Sensitive Data	RA-3, SA-8, SI-4	A.5.8, A.8.28	Privacy by design	CC3, CC7, P4	AI / Risk Mgmt
12	Healthcare Technology Provider Notice	45 CFR §164.520	Arts. 12–14	Notice / Transparency	PL-2	A.5.31	Transparency	CC2	Privacy Governance
13	No Practice of Medicine	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
14	No Practice of Psychology	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
15	No Psychotherapy Services	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
16	No Psychiatric Services	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
17	No Medical Diagnosis	N/A	Arts. 12–14, 22	Consumer Notice	PL-2, RA-3	A.5.31	Transparency	CC2, P1	Governance
18	No Medical Treatment	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
19	No Prescribing Services	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
20	No Provider-Patient Relationship	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
21	No Clinical Decision Replacement	HIPAA Security Rule where ePHI involved	Arts. 5, 22, 25, 35	Automated Decisioning	RA-3, SA-8	A.5.8, A.8.28	Privacy by design	CC3, P4	Risk Mgmt
22	Professional Judgment Requirement	N/A	Arts. 22, 25	Automated Decisioning	RA-3	A.5.8	Governance	CC3	AI Governance

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
23	User Responsibilities	45 CFR §164.308(a)(5)	Arts. 24, 32	Security Obligations	AT-2, AC-2	A.6.3, A.8.2	User obligations	CC6	Workforce Security
24	Not Emergency Services	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
25	Not Crisis Services	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
26	Not Suicide Prevention Services	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
26A	Not a 988 Replacement	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
27	Not a 911 Replacement	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
28	Not Emergency Dispatch	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance
29	Emergency Escalation Responsibilities	45 CFR §164.308(a)(5)	Arts. 24, 32	Security / Safety Notice	IR-4, CP-2	A.5.24, A.5.30	Incident governance	CC7, A1	Incident / Continuity
30	User Responsibilities During Emergencies	N/A	Arts. 12–14	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Governance

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
31	Provider Responsibilities During Emergencies	45 CFR §164.308(a)(5)	Arts. 24, 32	Security / Safety Notice	AT-2, IR-4	A.6.3, A.5.24	Role accountability	CC6, CC7	Workforce / Incident
32	Responsible AI Governance Program	HIPAA Security Rule where ePHI involved	Arts. 5, 22, 24, 25, 35	Automated Decisioning / Sensitive PI	PM-9, RA-3, SA-8	A.5.1, A.5.8	Privacy by design	CC1, CC3, P4	AI Risk Mgmt
33	Governance Objectives	45 CFR §164.308(a)(1)	Arts. 5, 24	Governance	PM-1, PM-9	A.5.1, A.5.2	Privacy governance	CC1, CC2	Governance
34	Governance Structure	45 CFR §164.308(a)(2)	Arts. 24, 25	Governance	PM-1, PM-2	A.5.2, A.5.4	Roles / accountability	CC1	Governance
35	AI Governance Committee	45 CFR §164.308(a)(2)	Arts. 24, 25, 35	Governance / Risk	PM-2, PM-9, RA-3	A.5.2, A.5.4	Privacy governance	CC1, CC3	Governance
36	Executive Oversight	45 CFR §164.308(a)(2)	Art. 24	Governance	PM-2, PM-9	A.5.2	Accountability	CC1	Governance
37	Clinical Oversight	HIPAA where PHI/ePHI involved	Arts. 22, 25, 35	Automated Decisioning	RA-3, SA-8	A.5.8	Risk governance	CC3, P4	Clinical AI Risk
38	Technical Oversight	45 CFR §164.308(a)(1), §164.312	Arts. 25, 32	Reasonable Security	SA-8, SI-4, CM-2	A.8.8, A.8.9, A.8.28	Security controls	CC6, CC7	Technical Security
39	Compliance Oversight	45 CFR §164.308(a)(1)	Arts. 24, 30, 35	Governance	CA-2, CA-7, PM-9	A.5.35, A.5.36	Compliance monitoring	CC2, CC4	Compliance

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
40	Privacy Oversight	45 CFR §164.308, §164.520	Arts. 5, 12–14, 24, 25, 35	Privacy Governance	PT-1, PT-2, AR-2	A.5.34	Privacy governance	P1, P2, P4	Privacy
41	Security Oversight	45 CFR §164.308(a)(1), §164.312	Arts. 25, 32	Reasonable Security	PM-9, RA-3, SI-4, IR-4	A.5.1, A.5.7, A.8.8	Security governance	CC6, CC7	Information Security
42	AI Risk Management Oversight	HIPAA Security Rule where ePHI involved	Arts. 22, 25, 32, 35	Automated Decisioning / Risk Assessment	RA-3, RA-7, PM-9, SA-8	A.5.8, A.8.28	Privacy risk mgmt	CC3, CC4, P4	AI Risk Management
43	Continuous Monitoring	45 CFR §164.308(a)(1)(ii)(D), §164.312(b)	Arts. 24, 32	Reasonable Security	CA-7, SI-4, AU-6	A.8.15, A.8.16	Monitoring	CC4, CC7	Monitoring
44	Continuous Improvement	45 CFR §164.308(a)(8)	Arts. 24, 32	Governance	CA-2, CA-7, PM-9	A.5.35, A.5.36	Management review	CC4	Corrective Action
45	Human Oversight Framework	HIPAA where PHI/ePHI involved	Arts. 5, 22, 24, 25, 35	Automated Decisioning	RA-3, SA-8, PL-2	A.5.8, A.5.31	Accountability	CC3, P4	AI Governance
46	Human-in-the-Loop	HIPAA where PHI/ePHI involved	Arts. 22, 25, 35	Automated Decisioning	SA-8, RA-3, AC-6	A.5.8, A.8.2	Human oversight	CC3, P4	AI Control
47	Human-on-the-Loop	HIPAA where PHI/ePHI involved	Arts. 22, 25, 32, 35	Automated Decisioning	CA-7, SI-4, RA-3	A.8.15, A.8.16	Monitoring	CC4, CC7, P4	Monitoring
48	Human-over-the-Loop	HIPAA where PHI/ePHI involved	Arts. 24, 25, 35	Governance / Risk	PM-9, RA-3, CA-2	A.5.1, A.5.2	Governance	CC1, CC3	Governance
49	Human Review Requirements	HIPAA where PHI/ePHI involved	Arts. 5, 22, 25	Automated Decisioning	RA-3, SA-8	A.5.8	Review controls	CC3, P4	AI Review
50	Documentation Review Requirements	45 CFR §164.312(b), §164.316(b)	Arts. 5, 24, 30	Records / Integrity	AU-2, AU-6, SI-7	A.5.33, A.8.15	Records mgmt	CC7, PI1	Documentation
51	Clinical Validation	HIPAA where PHI/ePHI involved	Arts. 22, 25, 35	Automated Decisioning	RA-3, SA-8, CA-2	A.5.8, A.8.28	Validation	CC3, P4	Clinical AI Risk

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
	Requirements								
52	Operational Validation Requirements	45 CFR §164.308(a)(8)	Arts. 24, 25, 32	Governance / Security	CA-2, CA-7, SA-11	A.8.29, A.8.32	Quality review	CC4, PI1	Quality Assurance
53	Escalation Requirements	45 CFR §164.308(a)(6)	Arts. 32, 33, 34	Incident Response	IR-4, IR-6, IR-8	A.5.24, A.5.25	Incident mgmt	CC7	Incident Management
54	Accountability Requirements	45 CFR §164.308(a)(2), §164.316	Arts. 5(2), 24, 30	Governance	PM-2, PM-9, PL-2	A.5.2, A.5.31	Accountability	CC1, CC2	Governance
55	Hallucinations	HIPAA where ePHI involved	Arts. 5, 22, 25, 35	Automated Decisioning	RA-3, SA-8	A.5.8	AI transparency	CC3, P4	AI Risk
56	Inaccuracies	HIPAA where ePHI involved	Arts. 5, 16, 22, 25	Correction / Automated Decisioning	RA-3, SI-7, SA-8	A.5.8, A.8.29	Accuracy	PI1, P4	Data Quality
57	Bias	N/A unless PHI/ePHI involved	Arts. 5, 22, 25, 35	Automated Decisioning / Sensitive PI	RA-3, RA-7, SA-8	A.5.8	Fairness / risk	CC3, P4	AI Fairness
58	Incomplete Context	HIPAA where ePHI involved	Arts. 5, 22, 25	Automated Decisioning	RA-3, SA-8	A.5.8	Data quality	CC3, P4	AI Risk
59	Missing Information	HIPAA where ePHI involved	Arts. 5, 16, 22, 25	Correction / Accuracy	SI-7, RA-3	A.5.33, A.8.29	Accuracy	PI1, P4	Data Quality
60	Model Drift	HIPAA where ePHI involved	Arts. 25, 32, 35	Risk Assessment	CA-7, RA-5, SI-4	A.8.8, A.8.16	Monitoring	CC4, CC7	Monitoring
61	Performance Degradation	45 CFR §164.308(a)(8) where ePHI involved	Arts. 25, 32	Reasonable Security	CA-7, SI-4, SA-11	A.8.16, A.8.29	Quality monitoring	CC4, A1	Availability / Quality
62	Regulatory Changes	45 CFR §164.308(a)(1)	Arts. 24, 25, 32	Governance	PM-9, PL-2, CA-2	A.5.31, A.5.36	Compliance monitoring	CC2, CC4	Compliance
63	Data Quality Limitations	HIPAA Privacy/Security	Arts. 5(1)(d), 16	Correction / Accuracy	SI-7, RA-3	A.5.33, A.8.29	Accuracy	PI1	Data Quality

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
		where PHI/ePHI involved							
64	Third-Party Dependencies	45 CFR §164.308(b), §164.314	Arts. 28, 32	Service Provider Controls	SA-9, SR-3, SR-5	A.5.19, A.5.20, A.5.21	Processor mgmt	CC9	Third Party Risk
65	User Notification	45 CFR §164.520	Arts. 12–14, 22	Notice / Automated Decisioning	PL-2, PT-1	A.5.31, A.5.34	Transparency	CC2, P1	Privacy Notice
66	Output Labeling	HIPAA where ePHI involved	Arts. 12–14, 22	Automated Decisioning Notice	PL-2, SA-8	A.5.31	Transparency	CC2, P4	AI Transparency
67	Explainability	HIPAA where ePHI involved	Arts. 13–15, 22	Automated Decisioning	SA-8, RA-3	A.5.8	Transparency	CC3, P4	AI Governance
68	Traceability	45 CFR §164.312(b), §164.316	Arts. 5(2), 24, 30	Governance / Records	AU-2, AU-6, AU-12	A.8.15, A.8.17	Accountability	CC7, P4	Audit Logging
69	Auditability	45 CFR §164.312(b), §164.308(a)(1)(ii)(D)	Arts. 5(2), 24, 30, 32	Governance / Security	AU-2, AU-6, CA-7	A.8.15, A.8.16	Audit controls	CC4, CC7	Audit
70	Decision Accountability	45 CFR §164.308(a)(2), §164.316	Arts. 5(2), 22, 24	Automated Decisioning	PM-2, PM-9, PL-2	A.5.2, A.5.31	Accountability	CC1, CC2, P4	Governance
71	AI Documentation	45 CFR §164.316(b)	Arts. 24, 30, 35	Records / Governance	PL-2, SA-5, AU-12	A.5.37, A.8.32	Documentation	CC2, CC3	Documentation
72	AI Records Retention	45 CFR §164.316(b)(2)(i)	Arts. 5, 30	Records / Retention	AU-11, SI-12	A.5.33, A.8.10	Retention	CC7, P5	Records Retention
73	Model Inventory	HIPAA Security Rule where ePHI involved	Arts. 24, 30, 35	Governance / Risk	CM-8, PM-5, SA-8	A.5.9, A.5.14	Inventory	CC3, CC6	Asset Mgmt
74	Model Validation	HIPAA where ePHI involved	Arts. 25, 32, 35	Risk Assessment	SA-11, CA-2, RA-3	A.8.29, A.8.32	Validation	CC3, PI1	Validation
75	Model Testing	HIPAA where ePHI involved	Arts. 25, 32, 35	Risk Assessment	SA-11, RA-5, CA-8	A.8.29, A.8.34	Testing	CC4, CC7	Testing

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
76	Model Monitoring	45 CFR §164.308(a)(1)(ii)(D)	Arts. 25, 32, 35	Risk Assessment	CA-7, SI-4, AU-6	A.8.15, A.8.16	Monitoring	CC4, CC7	Continuous Monitoring
77	Model Retirement	HIPAA where ePHI involved	Arts. 5, 25, 32	Governance / Retention	CM-3, SA-22, SI-12	A.8.10, A.8.32	Lifecycle mgmt	CC3, CC8	Lifecycle Mgmt
78	Change Management	45 CFR §164.308(a)(1), §164.312(c)	Arts. 25, 32	Reasonable Security	CM-3, CM-4, SA-10	A.8.32, A.8.9	Change mgmt	CC8	Change Control
79	Bias Assessments	N/A unless PHI/ePHI involved	Arts. 5, 22, 25, 35	Automated Decisioning / Sensitive PI	RA-3, RA-7, SA-8	A.5.8	Fairness / DPIA	CC3, P4	AI Risk
80	Safety Assessments	HIPAA where ePHI involved	Arts. 25, 32, 35	Risk Assessment	RA-3, SA-8, CA-2	A.5.8, A.8.28	Risk assessment	CC3, CC4	Safety / Risk
81	Quality Assurance	45 CFR §164.308(a)(8)	Arts. 24, 25, 32	Governance	CA-2, CA-7, SA-11	A.8.29, A.5.36	Quality review	CC4, PI1	Quality Mgmt
82	Incident Escalation	45 CFR §164.308(a)(6), §164.314	Arts. 33, 34	Breach / Security Notice	IR-4, IR-6, IR-8	A.5.24, A.5.25, A.5.26	Incident response	CC7	Incident Mgmt
83	Regulatory Monitoring	45 CFR §164.308(a)(1), §164.316	Arts. 24, 25, 32, 35	Governance / Compliance	PM-9, CA-2, PL-2	A.5.31, A.5.36	Compliance monitoring	CC2, CC4	Compliance
84	Data Collection	45 CFR §164.502, §164.506, §164.514	Arts. 5, 6, 9, 12–14	Notice at Collection / Sensitive PI	PT-1, PT-2, AR-2	A.5.34	Collection limitation	P1, P2	Privacy
85	Data Use	45 CFR §164.502, §164.506	Arts. 5, 6, 9	Use Limitation	PT-2, AR-4	A.5.34	Purpose specification	P2, P3	Privacy
86	Data Sharing	45 CFR §164.502, §164.508, §164.514, §164.524	Arts. 13–14, 28, 32	Disclosure / Service Provider	PT-7, SA-9, SR-3	A.5.19, A.5.20	Third-party disclosure	P4, CC9	Third Party / Privacy
87	Data Minimization	45 CFR §164.502(b)	Art. 5(1)(c)	Data Minimization Concepts	PT-2, PT-3	A.5.34	Data minimization	P3	Privacy
88	Purpose Limitation	45 CFR §164.502	Art. 5(1)(b)	Purpose Disclosure	PT-2	A.5.34	Purpose limitation	P2	Privacy

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
89	Data Quality	45 CFR §164.526	Art. 5(1)(d), Art. 16	Right to Correct	SI-7, PT-2	A.5.33	Accuracy	PI1, P2	Data Quality
90	Privacy Rights	45 CFR §164.520, §164.524, §164.526	Arts. 12–23	Consumer Rights	PT-1, PT-2, AR-8	A.5.34	Data subject rights	P1, P2	Privacy Rights
91	HIPAA Rights	45 CFR §164.520, §164.524, §164.526, §164.528	N/A	N/A	PT-1, AR-8	A.5.34	Rights management	P1	HIPAA Privacy
92	GDPR Rights	N/A	Arts. 12–23	N/A	PT-1, PT-2, AR-8	A.5.34	Data subject rights	P1, P2	Privacy Rights
93	California Rights	N/A	N/A	CCPA/CPRA Rights to Know, Delete, Correct, Limit, Opt-Out, Non-Discrimination	PT-1, PT-2, AR-8	A.5.34	Rights management	P1, P2	Privacy Rights
94	Consumer Health Data Rights	HIPAA where PHI involved	Arts. 12–23 where applicable	Consumer Health Privacy Laws / Sensitive PI	PT-1, PT-2, AR-8	A.5.34	Health data rights	P1, P2	Privacy
95	Cross-Border Transfers	45 CFR §164.314 where vendor involved	Arts. 44–49	Service Provider / Transfer Notices	SA-9, SR-3	A.5.19, A.5.20	Transfer controls	CC9, P4	Third Party / Privacy
96	Data Subject Requests	45 CFR §164.524, §164.526, §164.528	Arts. 12–23	Consumer Request Handling	PT-1, PT-2, AR-8	A.5.34	Rights handling	P1, P2	Privacy Rights
97	Consent Management	45 CFR §164.508 where authorization required	Arts. 6, 7, 9	Consent / Sensitive PI	PT-4, PT-5	A.5.34	Consent management	P2, P3	Consent
98	De-Identification	45 CFR §164.514(a)-(b)	Arts. 5, 25, 32	Deidentified Data	PT-2, PT-7	A.8.11	PII de-identification	P3, P4	Privacy

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
99	Anonymization	45 CFR §164.514 where applicable	Recital 26, Arts. 5, 25	Deidentified / Aggregated Data	PT-2, PT-7	A.8.11	Anonymization	P3	Privacy
100	Data Retention	45 CFR §164.316(b)(2)(i), §164.530(j)	Art. 5(1)(e), Art. 30	Retention Disclosure	SI-12, AU-11	A.5.33	Retention	P5	Records Retention
101	Data Deletion	HIPAA retention exceptions apply	Arts. 17, 5(1)(e)	Right to Delete	SI-12, MP-6	A.8.10, A.8.11	Disposal / deletion	P5	Disposal
102	Legal Holds	45 CFR §164.316(b), §164.530(j)	Arts. 17(3), 30	Legal Exceptions	SI-12, AU-11	A.5.33	Retention exceptions	P5	Legal Retention
103	Privacy Governance	45 CFR §164.308(a)(1), §164.530	Arts. 5(2), 24, 25, 35	Governance / Risk Assessment	PM-9, PT-1, RA-3	A.5.1, A.5.34	Privacy governance	P1, P2, CC1	Privacy Program
104	Security Governance	45 CFR §164.308(a)(1)(i), §164.308(a)(2)	Arts. 24, 32	Reasonable Security	PM-1, PM-9, PL-2	A.5.1, A.5.2	Security governance	CC1, CC2, CC6	InfoSec Program
105	Risk Management	45 CFR §164.308(a)(1)(ii)(A)-(B)	Arts. 25, 32, 35	Risk Assessment	RA-3, RA-7, PM-9	A.5.7, A.5.36	Risk assessment	CC3, CC4	Risk Mgmt
106	Asset Management	45 CFR §164.310(d), §164.312	Art. 32	Reasonable Security	CM-8, PM-5	A.5.9, A.5.10	Asset inventory	CC6	Asset Mgmt
107	Identity Management	45 CFR §164.308(a)(3), §164.312(a)	Art. 32	Security Controls	IA-2, IA-4, IA-5	A.5.16, A.5.17	Identity controls	CC6	IAM
108	Access Controls	45 CFR §164.312(a)(1), §164.308(a)(4)	Art. 32	Reasonable Security	AC-2, AC-3, AC-6	A.5.15, A.5.18, A.8.2	Access control	CC6	Access Control
109	Authentication	45 CFR §164.312(d)	Art. 32	Reasonable Security	IA-2, IA-5, IA-8	A.5.17, A.8.5	Authentication	CC6	Authentication
110	Authorization	45 CFR §164.312(a), §164.308(a)(4)	Art. 32	Reasonable Security	AC-3, AC-6	A.5.15, A.8.2	Authorization	CC6	Authorization

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
111	Encryption	45 CFR §164.312(a)(2)(iv), §164.312(e)(2)(ii)	Art. 32	Reasonable Security	SC-8, SC-13, SC-28	A.8.24	Cryptography	CC6, C1	Encryption
112	Logging	45 CFR §164.312(b)	Arts. 30, 32	Security Records	AU-2, AU-6, AU-12	A.8.15	Logging	CC7	Audit Logging
113	Security Monitoring	45 CFR §164.308(a)(1)(ii)(D), §164.312(b)	Art. 32	Reasonable Security	SI-4, CA-7, AU-6	A.8.16	Monitoring	CC7	Monitoring
114	SIEM	45 CFR §164.312(b), §164.308(a)(6)	Art. 32	Reasonable Security	AU-6, SI-4, IR-5	A.8.15, A.8.16	Security monitoring	CC7	Security Monitoring
115	Endpoint Security	45 CFR §164.308(a)(5), §164.312	Art. 32	Reasonable Security	SI-3, CM-7, AC-19	A.8.1, A.8.7	Endpoint controls	CC6, CC7	Endpoint Security
116	Vulnerability Management	45 CFR §164.308(a)(1)(ii)(A)-(B), §164.308(a)(8)	Art. 32	Reasonable Security	RA-5, SI-2, SI-4	A.8.8	Vulnerability mgmt	CC7	Vulnerability Mgmt
117	Patch Management	45 CFR §164.308(a)(1)(ii)(B), §164.312(c)	Art. 32	Reasonable Security	SI-2, CM-3, CM-4	A.8.8, A.8.9	Patch controls	CC7	Patch Mgmt
118	Secure Development	45 CFR §164.308(a)(1), §164.312(c)	Arts. 25, 32	Reasonable Security	SA-3, SA-8, SA-11	A.8.25, A.8.27, A.8.28, A.8.29	Privacy by design	CC3, CC8	SDLC
119	Penetration Testing	45 CFR §164.308(a)(8)	Art. 32	Reasonable Security	CA-8, RA-5	A.8.8, A.8.29	Testing	CC4, CC7	Security Testing
120	Cloud Security	45 CFR §164.308(b), §164.314(a), §164.312	Arts. 28, 32	Service Provider Security	SC-7, SA-9, SR-3	A.5.23, A.5.19, A.8.3	Processor controls	CC6, CC9	Cloud Security
121	Network Security	45 CFR §164.312(e), §164.312(a)	Art. 32	Reasonable Security	SC-7, AC-4, SI-4	A.8.20, A.8.21, A.8.22	Network controls	CC6, CC7	Network Security

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
122	Backup & Recovery	45 CFR §164.308(a)(7)(ii)(A), §164.310(a)(2)(i)	Art. 32	Reasonable Security	CP-9, CP-10	A.8.13	Backup controls	A1, CC7	Backup
123	Disaster Recovery	45 CFR §164.308(a)(7)(ii)(B)-(C)	Art. 32	Business Continuity	CP-2, CP-4, CP-10	A.5.29, A.5.30	Continuity	A1	Disaster Recovery
124	Business Continuity	45 CFR §164.308(a)(7)	Art. 32	Business Continuity	CP-2, CP-4	A.5.29, A.5.30	Continuity planning	A1	Business Continuity
125	Vendor Risk Management	45 CFR §164.308(b), §164.314(a)	Arts. 28, 32	Service Provider / Contractor	SA-9, SR-3, SR-5	A.5.19, A.5.20, A.5.21, A.5.22	Processor mgmt	CC9	Third Party Risk
126	Security Awareness & Training	45 CFR §164.308(a)(5)	Arts. 24, 32	Security Training	AT-2, AT-3	A.6.3	Awareness	CC2	Training
127	Incident Response	45 CFR §164.308(a)(6), §164.314(a)	Arts. 32, 33, 34	Breach Notification / Security	IR-1, IR-4, IR-6, IR-8	A.5.24, A.5.25, A.5.26, A.5.27	Incident response	CC7	Incident Mgmt
128	Responsible Disclosure	45 CFR §164.308(a)(6), §164.308(a)(8)	Arts. 32, 33	Reasonable Security	RA-5, IR-4, SI-2	A.5.24, A.8.8	Security incident support	CC7	Vulnerability Mgmt
129	Safe Harbor	45 CFR §164.308(a)(1), §164.308(a)(6)	Art. 32	Security Governance	RA-5, IR-4	A.5.24, A.8.8	Security governance	CC7	Security Governance
130	Reporting Requirements	45 CFR §164.308(a)(6)	Arts. 32, 33	Security Reporting	IR-6, IR-8	A.5.24, A.5.25	Incident reporting	CC7	Incident Mgmt
131	Submission Procedures	45 CFR §164.308(a)(6)	Arts. 32, 33	Security Reporting	IR-6, IR-8	A.5.24, A.5.25	Incident reporting	CC7	Incident Mgmt
132	Investigation Process	45 CFR §164.308(a)(6)(ii)	Arts. 32, 33, 34	Breach / Security Investigation	IR-4, IR-5, IR-6	A.5.25, A.5.26	Incident investigation	CC7	Incident Mgmt
133	Severity Ratings	45 CFR §164.308(a)(6), §164.308(a)(1)	Arts. 32, 33	Risk-Based Security	RA-3, RA-5, IR-4	A.5.7, A.8.8	Risk classification	CC3, CC7	Risk Mgmt

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
134	Remediation Lifecycle	45 CFR §164.308(a)(1)(ii)(B), §164.308(a)(8)	Art. 32	Reasonable Security	RA-5, SI-2, IR-4	A.8.8, A.5.25	Corrective action	CC4, CC7	Remediation
135	Coordinated Disclosure	45 CFR §164.308(a)(6)	Arts. 32, 33, 34	Security Notice	IR-6, IR-8	A.5.24, A.5.27	Communications	CC7	Incident Comms
136	Researcher Recognition	N/A	N/A	N/A	PM-9	A.5.1	Governance	CC1	Governance
137	Security Communications	45 CFR §164.308(a)(6), §164.314	Arts. 32, 33, 34	Security Notice / Breach Notice	IR-6, IR-8	A.5.24, A.5.27	Incident communication	CC7	Incident Comms
138	Accessibility Governance	N/A	Art. 25 where digital access/privacy by design applies	Consumer Access / Non-Discrimination Principles	PL-2, PM-9	A.5.1, A.5.31	Governance	CC1, CC2	Governance
139	Accessibility Program Objectives	N/A	Art. 25	Consumer Access	PL-2, SA-8	A.5.31	Design governance	CC2	Governance
140	ADA Commitment	N/A	N/A	Consumer Access / Non-Discrimination Principles	PL-2	A.5.31	Transparency	CC2	Governance
141	WCAG 2.2 Alignment	N/A	Art. 25 where applicable	Consumer Access	SA-8, PL-2	A.5.31, A.8.29	Privacy by design	CC2	Accessibility
142	Section 508 Alignment	N/A	N/A	Public Sector Accessibility	SA-8, PL-2	A.5.31	Design governance	CC2	Accessibility
143	Accessible Product Design	N/A	Art. 25	Consumer Access	SA-8, SA-11	A.8.25, A.8.29	Privacy by design	CC3	Product Governance
144	Accessibility Testing Program	N/A	Art. 25	Consumer Access	SA-11, CA-2	A.8.29, A.8.34	Testing	CC4	Testing

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
145	Accessibility Reviews	N/A	Art. 25	Consumer Access	CA-2, SA-11	A.8.29	Review controls	CC4	Review
146	Accessibility Issue Management	N/A	Art. 25	Consumer Access	SI-2, CA-2	A.8.8, A.5.35	Corrective action	CC4	Issue Mgmt
147	Accessibility Roadmap	N/A	Art. 25	Consumer Access	PM-9, PL-2	A.5.1, A.5.31	Governance planning	CC1, CC2	Governance
148	User Feedback	N/A	Arts. 12–14 where applicable	Consumer Requests	IR-6, PL-2	A.5.27, A.5.31	Feedback handling	CC2	Communications
149	Accommodation Requests	N/A	Arts. 12–14 where applicable	Consumer Access	PL-2, IR-6	A.5.31	Request management	CC2	Request Mgmt
150	Third-Party Accessibility	N/A	Art. 28 where vendors process data	Service Provider / Vendor	SA-9, SR-3	A.5.19, A.5.20	Processor/vendor mgmt	CC9	Third Party Risk
151	Continuous Improvement	45 CFR §164.308(a)(8) where security/privacy related	Arts. 24, 25, 32	Governance	CA-2, CA-7, PM-9	A.5.35, A.5.36	Management review	CC4	Corrective Action
152	IP Overview	N/A	N/A	N/A	PL-2	A.5.32	N/A	CC2	Governance
153	Trademarks	N/A	N/A	N/A	PL-2	A.5.32	N/A	CC2	Legal Governance
154	Copyrights	N/A	N/A	N/A	PL-2	A.5.32	N/A	CC2	Legal Governance
155	Proprietary Technology	45 CFR §164.308(a)(1) where security controls involved	Art. 32 where processing tech involved	Reasonable Security	SA-8, SA-10, CM-8	A.5.9, A.5.32	Processor systems	CC6, CC8	Asset Protection
156	AI Models	HIPAA where PHI/ePHI involved	Arts. 22, 25, 32, 35	Automated Decisioning	SA-8, RA-3, CM-8	A.5.8, A.5.9	AI governance	CC3, P4	AI Risk Mgmt

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
157	Algorithms	HIPAA where PHI/ePHI involved	Arts. 22, 25, 32	Automated Decisioning	SA-8, RA-3	A.5.8	AI governance	CC3, P4	AI Governance
158	Source Code	45 CFR §164.308(a)(1), §164.312(c)	Art. 32	Reasonable Security	SA-10, SA-11, CM-5	A.8.4, A.8.25, A.8.28	Security by design	CC6, CC8	Secure SDLC
159	Documentation	45 CFR §164.316(b) where HIPAA controls involved	Arts. 24, 30	Records / Governance	PL-2, SA-5	A.5.37	Documentation	CC2	Documentation
160	Platform Rights	N/A unless data/security controls involved	N/A	N/A	PL-2, SA-5	A.5.32	N/A	CC2	Legal Governance
161	Customer Data Ownership	45 CFR §164.524, §164.526, §164.530	Arts. 5, 15–17, 20	Access / Deletion / Correction	PT-1, PT-2, AR-8	A.5.34	Data subject rights	P1, P2	Privacy Rights
162	Feedback Rights	N/A	Arts. 12–14 if personal data included	Notice / Use	PL-2, PT-2	A.5.31	Transparency	CC2	Governance
163	Open Source Components	45 CFR §164.308(a)(1) where security risk involved	Art. 32	Reasonable Security	SA-10, SA-15, RA-5	A.8.8, A.8.25	Supplier/software risk	CC8, CC9	Software Supply Chain
164	Restrictions	45 CFR §164.308(a)(4), §164.312(a)	Art. 32	Security Obligations	AC-3, AC-6, CM-5	A.5.15, A.8.2, A.8.4	Access restrictions	CC6	Access Control
165	Reservation of Rights	N/A	N/A	N/A	PL-2	A.5.32	N/A	CC2	Legal Governance
166	Enforcement	45 CFR §164.308(a)(1), §164.308(a)(5)	Arts. 24, 32	Governance / Security Enforcement	PL-4, IR-4, PS-8	A.5.1, A.6.4	Enforcement governance	CC1, CC2	Governance
167	Acceptable Use Purpose	45 CFR §164.308(a)(5)	Arts. 24, 32	Security Obligations	PL-4, AT-2	A.5.10, A.6.3	User obligations	CC2, CC6	Acceptable Use
168	Prohibited Activities	45 CFR §164.308(a)(5), §164.312(a)	Art. 32	Security Obligations	PL-4, AC-6	A.5.10, A.5.15	User obligations	CC6	Acceptable Use

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
169	Security Violations	45 CFR §164.308(a)(6), §164.312	Arts. 32, 33	Security Incident	IR-4, IR-6, AC-6	A.5.24, A.5.25	Incident mgmt	CC7	Incident Mgmt
170	Data Misuse	45 CFR §164.502, §164.308(a)(4)	Arts. 5, 6, 32	Unauthorized Use / Disclosure	AC-3, PT-2, IR-4	A.5.10, A.5.15, A.5.34	Data use limitation	P2, CC6	Privacy / Access
171	AI Misuse	HIPAA where PHI/ePHI involved	Arts. 22, 25, 32, 35	Automated Decisioning / Security	RA-3, SA-8, PL-4	A.5.8, A.5.10	AI governance	CC3, P4	AI Governance
172	Reverse Engineering	45 CFR §164.308(a)(1) where security implicated	Art. 32	Security / IP	CM-5, SA-10	A.5.32, A.8.4	Security controls	CC6, CC8	Asset Protection
173	Automated Scraping	45 CFR §164.308(a)(1), §164.312(a)	Arts. 5, 32	Data Misuse / Security	AC-6, SC-5, SI-4	A.8.16, A.8.20	Data protection	CC6, CC7	Abuse Prevention
174	Abuse Prevention	45 CFR §164.308(a)(1), §164.312	Arts. 32, 33	Security / Fraud Prevention	SI-4, IR-4, AU-6	A.8.16, A.5.24	Monitoring	CC7	Abuse Monitoring
175	User Conduct Standards	45 CFR §164.308(a)(5)	Arts. 24, 32	Security / Conduct	AT-2, PL-4	A.6.3, A.5.10	User obligations	CC2, CC6	Training / Conduct
176	Platform Integrity Protections	45 CFR §164.312(c), §164.312(e)	Art. 32	Reasonable Security	SI-7, SC-7, SI-4	A.8.16, A.8.20, A.8.21	Integrity controls	CC6, CC7, PI1	Integrity
177	Enforcement Actions	45 CFR §164.308(a)(1), §164.308(a)(5)	Arts. 24, 32	Enforcement / Security	PL-4, IR-4, PS-8	A.6.4, A.5.24	Enforcement	CC1, CC2	Governance
178	Suspension Criteria	45 CFR §164.308(a)(1), §164.312(a)	Art. 32	Security Enforcement	AC-2, AC-3, IR-4	A.5.18, A.5.24	Access restriction	CC6, CC7	Access / Incident
179	Reporting Misuse	45 CFR §164.308(a)(6), §164.308(a)(5)	Arts. 32, 33	Security Reporting	IR-6, AT-2	A.5.24, A.6.3	Incident reporting	CC7	Incident Reporting
180	Regulatory Compliance Overview	45 CFR §164.308(a)(1), §164.316	Arts. 5, 24, 30, 32	Governance / Compliance	PM-1, PM-9, PL-2	A.5.1, A.5.31, A.5.36	Privacy governance	CC1, CC2, CC4	Compliance Governance

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
181	HIPAA Alignment	45 CFR Parts 160, 162, 164	N/A	N/A	PL-2, RA-3, CA-2	A.5.31, A.5.36	Compliance mapping	CC2, CC4	HIPAA Controls
182	HITECH Alignment	HITECH Act; 45 CFR §164.400–414	N/A	N/A	IR-4, IR-6, IR-8	A.5.24, A.5.25, A.5.26	Breach governance	CC7	Breach Notification
183	GDPR Alignment	N/A	Arts. 5, 6, 9, 12–23, 24, 25, 28, 30, 32, 33, 34, 35, 44–49	N/A	PT-1, PT-2, RA-3	A.5.34, A.5.36	GDPR privacy governance	P1, P2, P4	Privacy Compliance
184	UK GDPR Alignment	N/A	UK GDPR Arts. 5, 6, 9, 12–23, 24, 25, 28, 30, 32, 33, 34, 35, 44–49	N/A	PT-1, PT-2, RA-3	A.5.34, A.5.36	UK privacy governance	P1, P2, P4	Privacy Compliance
185	CCPA Alignment	N/A	N/A	Cal. Civ. Code §1798.100, §1798.105, §1798.110, §1798.115, §1798.125, §1798.130	PT-1, PT-2, AR-8	A.5.34	Consumer rights	P1, P2	Consumer Privacy
186	CPRA Alignment	N/A	N/A	Cal. Civ. Code §1798.100, §1798.106, §1798.121, §1798.135, §1798.185	PT-1, PT-2, RA-3	A.5.34, A.5.36	Sensitive PI governance	P1, P2, P4	Consumer Privacy
187	Consumer Health Privacy Laws	HIPAA where PHI applies	Arts. 5, 6, 9 where applicable	Sensitive PI / Consumer Health Data	PT-1, PT-2, PT-4	A.5.34	Health data governance	P1, P2	Consumer Health Privacy
188	Telehealth Laws	HIPAA Privacy/Security where PHI/ePHI involved	Arts. 5, 6, 9, 32	Consumer Notice / Sensitive PI	PL-2, RA-3, AC-2	A.5.31, A.5.34	Processing transparency	CC2, P1	Telehealth Governance

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
189	NIST AI RMF Alignment	HIPAA where ePHI involved	Arts. 22, 25, 35	Automated Decisioning / Risk	RA-3, RA-7, SA-8, PM-9	A.5.8, A.5.36	AI/privacy risk	CC3, CC4, P4	AI Risk Mgmt
190	NIST CSF Alignment	45 CFR §164.308, §164.312	Art. 32	Reasonable Security	PM-9, RA-3, SI-4, IR-4, CP-2	A.5.1, A.8.16, A.5.24	Security governance	CC6, CC7, A1	Cybersecurity
191	NIST SP 800-53 Alignment	45 CFR §164.308, §164.312, §164.316	Arts. 24, 32	Reasonable Security	AC, AU, AT, CA, CM, CP, IA, IR, RA, SA, SC, SI	A.5, A.6, A.8 families	Security/privacy controls	CC1–CC9, A1, C1, P	Control Framework
192	ISO 27001 Alignment	45 CFR §164.308(a)(1)	Art. 32	Reasonable Security	PM-1, RA-3, CA-2	A.5.1, A.5.7, A.5.36, A.8 controls	Security governance	CC1, CC6, CC7	ISMS
193	ISO 27701 Alignment	45 CFR §164.520, §164.524, §164.526	Arts. 5, 12–23, 24, 25, 28, 30	Consumer Rights / Privacy Governance	PT-1, PT-2, AR-8	A.5.34	PIMS controls	P1, P2, P4	Privacy Management
194	HITRUST CSF Alignment	HIPAA / HITECH alignment	Arts. 24, 32 where applicable	Reasonable Security / Privacy	RA-3, AC-2, AU-6, IR-4, CP-2	A.5, A.6, A.8 controls	Privacy/security governance	CC1–CC9, A1, C1, P	HITRUST Domains
195	SOC 2 Alignment	HIPAA where applicable	Arts. 24, 32	Reasonable Security	CA-2, CA-7, PM-9	A.5.36, A.8.16	Trust services alignment	Security, Availability, Processing Integrity, Confidentiality, Privacy	Assurance Readiness
196	Future Regulatory Monitoring	45 CFR §164.308(a)(1), §164.316	Arts. 24, 25, 32, 35	Governance / Future Rulemaking	PM-9, CA-2, PL-2	A.5.31, A.5.36	Compliance monitoring	CC2, CC4	Compliance Monitoring

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
197	Disclaimer of Warranties	N/A	Arts. 12–14 where user notice applies	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Legal Governance
198	Limitation of Liability	N/A	Arts. 12–14 where user notice applies	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Legal Governance
199	Indemnification	45 CFR §164.314 where customer obligations apply	Arts. 28, 32 where processor terms apply	Service Provider / Contractor Terms	SA-9, SR-3	A.5.19, A.5.20	Processor contracts	CC9	Contract Governance
200	Force Majeure	45 CFR §164.308(a)(7) where continuity impacted	Art. 32	Business Continuity	CP-2, CP-10	A.5.29, A.5.30	Continuity	A1	Continuity
201	Suspension Rights	45 CFR §164.308(a)(1), §164.312(a)	Art. 32	Security Enforcement	AC-2, AC-3, IR-4	A.5.18, A.5.24	Access restriction	CC6, CC7	Access / Incident
202	Termination Rights	45 CFR §164.310(d), §164.316(b) where data retention applies	Arts. 17, 28, 30	Deletion / Service Provider Terms	AC-2, SI-12, SA-9	A.5.18, A.8.10	Termination / deletion	CC6, P5	Access / Retention
203	Export Controls	N/A	N/A	N/A	PL-2, SA-9	A.5.31	Legal compliance	CC2	Legal Compliance
204	Sanctions Compliance	N/A	N/A	N/A	PL-2, SA-9	A.5.31	Legal compliance	CC2	Legal Compliance
205	Assignment	45 CFR §164.314 where BAA/vendor obligations apply	Art. 28 where processor/subprocessor involved	Service Provider / Contractor Terms	SA-9, SR-3	A.5.19, A.5.20	Processor contracts	CC9	Third Party Governance
206	Governing Law	N/A	Arts. 12–14 where	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Legal Governance

Section	Framework Area	HIPAA	GDPR / UK GDPR	CCPA / CPRA	NIST SP 800-53	ISO 27001 Annex A	ISO 27701	SOC 2 TSC	HITRUST CSF
			notice applies						
207	Dispute Resolution	N/A	Arts. 12–14 where notice applies	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Legal Governance
208	Class Action Waiver	N/A	Arts. 12–14 where notice applies	Consumer Notice	PL-2	A.5.31	Transparency	CC2	Legal Governance
209	Severability	N/A	N/A	N/A	PL-2	A.5.31	Governance	CC2	Legal Governance
210	Entire Agreement	45 CFR §164.314 where contractual hierarchy applies	Art. 28 where processor terms apply	Service Provider Terms	SA-9, PL-2	A.5.19, A.5.20	Contract governance	CC2, CC9	Contract Governance
211	Changes to Framework	45 CFR §164.520, §164.316	Arts. 12–14, 24	Notice Updates	PL-2, PM-9	A.5.31, A.5.36	Notice governance	CC2, CC4	Governance Updates
212	Contact Information	45 CFR §164.520, §164.524	Arts. 12–14, 15–22	Consumer Request Contact	PT-1, IR-6	A.5.34	Data subject contact	P1, P2	Privacy Communications

E.2 MATRIX MAINTENANCE REQUIREMENTS

E.2.1 Periodic Review

This Section-by-Control Traceability Matrix should be reviewed periodically to confirm continued alignment with current governance practices, regulatory requirements, contractual obligations, operational controls, and product functionality.

Review should occur at least annually and additionally when material changes occur to:

- Cognera Health products or services
- AI-enabled functionality
- Security controls
- Privacy obligations
- Regulatory requirements
- Customer contractual commitments
- Vendor relationships
- Data processing activities
- Incident response procedures
- Business continuity requirements

E.2.2 Control Evidence

Each mapped section should be supported by appropriate evidence, which shall include:

- Policies
- Procedures
- Technical standards
- Risk assessments
- Security assessments
- Privacy impact assessments
- AI governance reviews
- Vendor assessments
- Training records
- Audit logs
- Incident records
- Access reviews
- Change management records
- Penetration testing reports
- Vulnerability management records

- Business continuity test results

E.2.3 Mapping Limitations

This matrix provides governance-level traceability and does not, by itself, prove implementation, operational effectiveness, certification, regulatory compliance, or audit readiness.

Final compliance determinations require review of:

- Actual implemented controls
- Operational evidence
- System architecture
- Customer contracts
- Data flows
- Risk assessments
- Legal analysis
- Independent audit results
- Regulatory requirements

E.2.4 Recommended Companion Artifact

Cognera Health should maintain this matrix in spreadsheet format with the following columns:

- Framework Section Number
- Framework Section Title
- Control Objective
- HIPAA Citation
- HITECH Citation
- GDPR Article
- UK GDPR Article
- CCPA/CPRA Reference
- Consumer Health Privacy Law Reference
- NIST AI RMF Function
- NIST CSF Function
- NIST SP 800-53 Control
- ISO 27001 Annex A Control
- ISO 27701 Control
- HITRUST CSF Control

- SOC 2 Trust Services Criteria
- Control Owner
- Evidence Type
- Review Frequency
- Implementation Status
- Notes

This spreadsheet should serve as the operational control traceability register supporting enterprise customer due diligence, audit preparation, health system procurement, investor review, and internal governance oversight.

APPENDIX F – IMPLEMENTATION, EVIDENCE & REVIEW REGISTER

F.1 Purpose

This Appendix establishes the operational register used to maintain evidence, ownership, review cadence, implementation status, and continuous improvement activities for the Cognera Health™ governance framework.

F.2 Evidence Categories

Evidence shall include:

- Policies
- Procedures
- Risk assessments
- Privacy impact assessments
- Security assessments
- AI governance reviews
- Access reviews
- Audit logs
- Incident reports
- Vulnerability scans
- Penetration test reports
- Vendor reviews
- Training records
- Business continuity tests
- Disaster recovery tests
- Accessibility reviews

- Change management records

F.3 Control Ownership

Each control should have an assigned owner, such as:

- Privacy Officer
- Security Officer
- Compliance Lead
- AI Governance Lead
- Product Owner
- Engineering Lead
- Clinical Advisor
- Operations Lead
- Legal Counsel
- Accessibility Lead

F.4 Review Frequency

Controls should be reviewed based on risk:

- Critical controls: quarterly or event-driven
- High-risk controls: semi-annually
- Standard controls: annually
- Legal/regulatory controls: upon regulatory change
- Incident-related controls: after each material incident

F.5 Implementation Status

Each control should be tracked as:

- Planned
- In Progress
- Implemented
- Partially Implemented
- Needs Remediation
- Under Review
- Retired

F.6 Corrective Action Tracking

Corrective actions should include:

- Issue description
- Risk rating
- Control owner
- Remediation plan
- Target completion date
- Evidence required
- Validation method
- Closure approval

F.7 Governance Reporting

Periodic governance reporting should summarize:

- Open risks
- Control gaps
- Remediation progress
- Security events
- Privacy events
- AI governance findings
- Accessibility findings
- Vendor risks
- Regulatory updates
- Audit readiness status

F.8 Continuous Improvement

Cognera Health should use evidence, reviews, incidents, audit findings, customer feedback, regulatory changes, and operational lessons learned to improve the framework over time.

Continuous improvement activities shall include:

- Policy updates
- Procedure updates
- Control enhancements
- Training updates
- Technical improvements
- Governance committee reviews
- Vendor control improvements
- Product design improvements

APPENDIX G – FINAL GOVERNANCE ATTESTATION STATEMENT

Cognera Health™ maintains this Platform Governance, Terms, Security, Privacy, Accessibility & Responsible AI Framework as a living governance document.

This Framework is intended to support transparency, accountability, privacy protection, security, responsible AI, accessibility, regulatory alignment, enterprise readiness, and continuous improvement.

This Framework does not constitute a legal opinion, certification, audit report, regulatory approval, or guarantee of compliance.

Cognera Health shall update this Framework periodically to reflect changes in technology, law, regulation, security practices, privacy expectations, AI governance, accessibility standards, customer requirements, operational maturity, and organizational practices.

Approved By: _____

Title: _____

Date: _____