CONFIDENTIAL | PROPRIETARY | RESTRICTED

Cognera Health
Data Retention, Deletion, and Secure Disposal Policy

NOTICE OF CONFIDENTIALITY

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

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

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

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

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

Any unauthorized use may result in:

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

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

Document Version Table

Version	Date	Author	Description
Draft 1.0	02/12/2026	John Budala	Initial draft created.

Table of Contents

1. Introduction

Cognera Health provides cloud-based healthcare Software-as-a-Service (SaaS) solutions, including HealScript™, HealConnect™ and associated services supporting mental health, behavioral health, wellness, well-being, integrated care, care coordination, clinical operations, and continuous care delivery.

As a Business Associate (BA) under the Health Insurance Portability and Accountability Act (HIPAA), Cognera Health processes, stores, transmits, analyzes, and protects Protected Health Information (PHI), electronic Protected Health Information (ePHI), Personal Information (PI), Personal Data, Consumer Health Data, and other sensitive information on behalf of Covered Entities and authorized customers.

This Data Retention, Deletion, and Secure Disposal Policy establishes governance, procedures, controls, and accountability mechanisms governing the lifecycle management of information from creation, collection, acquisition, storage, use, disclosure, retention, archival, deletion, destruction, anonymization, and final disposition.

The objectives of this policy are to:

- Ensure compliance with applicable privacy, security, healthcare, and data protection regulations.
- Reduce regulatory, legal, operational, cybersecurity, and privacy risks.
- Support data minimization and purpose limitation principles.
- Establish defensible retention schedules.
- Protect individual privacy rights.
- Enable secure destruction of information that is no longer required.
- Maintain audit readiness and regulatory compliance.
- Support continuity of care and clinical record preservation requirements.

1.1 Scope and Applicability

This policy applies to all Cognera Health™ platforms, applications, services, integrations, infrastructure, personnel, third-party providers, and operational activities, including HealScript™, HealConnect™, APIs, analytics, reporting, clinical intelligence, operational intelligence, and enterprise intelligence systems.

The policy applies to all employees, contractors, consultants, temporary personnel, interns, volunteers, vendors, Business Associates, subcontractors, and other authorized parties who access, process, store, transmit, or manage information on behalf of Cognera Health.

This policy governs the lifecycle management, protection, retention, deletion, and secure disposal of all regulated, confidential, operational, clinical, security, and business information, including Protected Health Information (PHI), electronic Protected Health Information (ePHI), personal information, consumer health data, clinical records, assessments, treatment documentation, communications, voice and audio records, audit and security logs, artificial intelligence governance records, analytics data, operational data, backup data, and archived information.

1.2 Regulatory and Standards Alignment

This policy supports alignment with applicable requirements arising from applicable healthcare regulations, privacy laws, cybersecurity standards, records management requirements, and industry-recognized governance frameworks.

United States Healthcare, Privacy, and Security Regulations

- HIPAA Privacy Rule (45 CFR Part 160 and Part 164)
- HIPAA Security Rule (45 CFR §164.302–318)
- HIPAA Breach Notification Rule (45 CFR §164.400–414)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Federal Trade Commission (FTC) requirements
- State Healthcare Record Retention Laws
- State Breach Notification Laws
- State Consumer Protection Laws
- State Healthcare Privacy Laws
- State Consumer Health Privacy Laws
- Applicable Telehealth and Behavioral Health Regulations

United States Consumer Privacy Regulations

Where applicable, Cognera Health incorporates privacy governance, records management, retention, deletion, and consumer rights requirements informed by:

- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Applicable U.S. State Privacy Laws
- Applicable Consumer Health Data Privacy Laws

Cognera Health supports privacy principles including:

- Transparency
- Purpose Limitation
- Data Minimization
- Storage Limitation

- Accuracy
- Accountability
- Consumer Access Rights
- Consumer Correction Rights
- Consumer Deletion Rights
- Consumer Data Portability Rights
- Sensitive Personal Information Protections
- Non-Discrimination Requirements

International Privacy and Data Protection Regulations

Where applicable, Cognera Health incorporates governance controls informed by:

- General Data Protection Regulation (GDPR)
- UK General Data Protection Regulation (UK GDPR)
- Other applicable international privacy and data protection regulations
- Cognera Health supports privacy principles including:
- Lawfulness, Fairness, and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability
- Individual Privacy Rights
- Responsible Data Stewardship

Security, Compliance, and Information Governance Frameworks

Cognera Health aligns its retention, deletion, destruction, and information lifecycle management practices with recognized industry frameworks including:

- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001 Information Security Management Systems
- ISO/IEC 27701 Privacy Information Management Systems
- SOC 2 Trust Services Criteria
- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 Security and Privacy Controls
- NIST SP 800-66 HIPAA Security Rule Guidance
- NIST SP 800-88 Rev.1 Media Sanitization Guidelines
- Center for Internet Security (CIS) Controls

These frameworks support the implementation of administrative, technical, operational, privacy, security, retention, deletion, legal hold, records management, and secure disposal controls throughout the information lifecycle.

2. Governance Structure

2.1 Privacy Officer

- **Role**: Oversees enterprise privacy, data protection, retention, deletion, and secure disposal programs.
- **Reporting**: Reports to the Chief Information Security Officer (CISO).
- **Responsibilities**:
    - Establish retention and disposal policies.
    - Review privacy rights requests.
    - Coordinate GDPR and CCPA compliance.
    - Review deletion requests.
    - Approve anonymization initiatives.
    - Coordinate legal hold activities.
    - Oversee regulatory reporting.
    - Conduct annual retention reviews.
    - Present quarterly privacy compliance reports.
- **Qualifications**: Certified in Healthcare Privacy Compliance (CHPC) or equivalent, with five years of experience in HIPAA, healthcare IT, and SaaS.
- **Delegation**: In absence, the backup officer assumes duties with notification to the CISO and Data Governance Steering Committee.

2.2 Data Governance Steering Committee

- **Composition**: Senior leaders from Privacy, Compliance, Information Security, Legal, Product Development, Operations, Engineering, Clinical Services, and other business functions responsible for information governance, privacy, security, compliance, and risk management .
- **Responsibilities**:
    - Approve data governance, retention, deletion, privacy, and information management policies annually or following significant regulatory, contractual, operational, or organizational changes.
    - Oversee compliance with applicable healthcare, privacy, cybersecurity, artificial intelligence, and information governance requirements, including HIPAA, HITECH, GDPR, UK GDPR, CCPA/CPRA, HITRUST, ISO 27001, ISO 27701, and related regulatory frameworks.
    - Review data lifecycle management practices, retention schedules, secure disposal methodologies, legal hold requirements, and data minimization initiatives.
    - Evaluate privacy controls, security controls, governance practices, compliance metrics, audit findings, risk assessments, and corrective action plans.

  - Oversee enterprise information governance, data protection, AI governance, records management, and regulatory readiness initiatives.
  - Allocate resources and establish priorities for privacy, security, compliance, risk management, and governance programs.
- **Meetings**: Quarterly, with ad-hoc sessions convened as necessary to address significant regulatory developments, audit findings, security incidents, privacy matters, compliance concerns, legal requirements, or other critical governance issues.

2.3 Legal and Regulatory Oversight

Policy: Cognera Health shall maintain ongoing oversight of evolving privacy, healthcare, cybersecurity, records management, and data protection regulations.

Procedures

- Review legal requirements annually.
- Monitor OCR (Office for Civil Rights) guidance.
- Monitor HHS (U.S. Department of Health and Human Services) guidance.
- Monitor GDPR developments.
- Monitor state privacy laws.
- Update retention schedules following material legal changes.
- Document all retention-related legal interpretations

3. Data Lifecycle Governance

3.1 Data Lifecycle Management Policy

- **Policy**: Cognera Health shall manage information throughout its lifecycle from collection through secure disposal in accordance with HIPAA, HITECH, GDPR, CCPA/CPRA, HITRUST, ISO 27001, ISO 27701, SOC 2, and applicable legal requirements.

- Data lifecycle:
  - Data Collection and Acquisition
  - Data Creation and Generation
  - Data Classification and Identification
  - Data Processing and Transformation
  - Data Storage and Preservation
  - Data Access and Retrieval
  - Data Use and Operational Utilization
  - Data Sharing and Exchange
  - Data Disclosure and Distribution
  - Data Archival and Long-Term Preservation
  - Data Retention and Records Management
  - Data Review and Disposition Assessment

- Data Deletion and Removal
- Data Destruction and Secure Disposal
- Data De-Identification and Anonymization
- Final Disposition and Lifecycle Closure

- **Procedures**: To ensure effective lifecycle management and regulatory compliance, Cognera Health shall:

  - Maintain and periodically review enterprise information and data inventories.
  - Classify information assets according to sensitivity, regulatory requirements, business value, and risk.
  - Establish and maintain approved retention schedules and disposition requirements.
  - Implement appropriate access controls, authentication mechanisms, and authorization procedures.
  - Apply encryption and other technical safeguards to protect sensitive information at rest, in transit, and during processing.
  - Monitor information access, usage, transmission, sharing, and disclosure activities.
  - Maintain audit trails and logging mechanisms to support accountability, traceability, and compliance monitoring.
  - Conduct periodic reviews of retention schedules, legal hold requirements, and disposition eligibility.
  - Document data deletion, de-identification, anonymization, and destruction activities.
  - Validate and verify secure destruction and disposal activities using approved methodologies.
  - Maintain evidence of retention, deletion, destruction, and final disposition activities in accordance with applicable regulatory, legal, contractual, and organizational requirements.
  - Periodically assess lifecycle management controls as part of compliance, privacy, security, risk management, and governance reviews.

3.2 Data Classification and Categorization

- **Policy:** Cognera Health shall classify information assets according to their sensitivity, regulatory requirements, business value, confidentiality requirements, operational impact, and risk profile. Data classification supports appropriate privacy, security, access control, retention, monitoring, and disposal requirements throughout the information lifecycle.
- **Classification Levels:**
  - **Restricted:** Restricted information represents the highest level of sensitivity and requires the strongest administrative, technical, and organizational safeguards.
    Examples:
    - Protected Health Information (PHI)
    - Electronic Protected Health Information (ePHI)
    - Mental Health Records
    - Behavioral Health Records

- Substance Use Disorder Records
- Crisis Intervention Records
- Clinical Documentation
- Treatment Plans
- Assessment Data
- Personally Identifiable Information (PII)
- Consumer Health Data
- Authentication Credentials
- Security Incident Records

- **Confidential:** Confidential information includes sensitive business, operational, legal, financial, security, and proprietary information intended for authorized personnel only.
  Examples:
  - Internal Business Records
  - Contracts and Agreements
  - Financial Records
  - Vendor Information
  - Compliance Documentation
  - Security Documentation
  - Risk Assessments
  - Audit Reports
  - Product Roadmaps
  - Proprietary Business Information
- **Internal Use:** Internal information is intended for use within Cognera Health and is not approved for public disclosure.
  Examples:
  - Internal Communications
  - Operational Procedures
  - Project Documentation
  - Training Materials
  - Internal Reports
  - Administrative Records
- **Public:** Public information is approved for public disclosure and may be shared without restriction.
  Examples:
  - Marketing Materials
  - Public Website Content
  - Published Reports
  - Press Releases
  - Public Announcements

- Publicly Available Documentation

3.3 Data Ownership and Stewardship

Policy: Cognera Health shall establish and maintain clear ownership, stewardship, accountability, and governance responsibilities for all information assets throughout their lifecycle to support privacy, security, compliance, risk management, operational effectiveness, and regulatory requirements.

Data owners are responsible for ensuring that information assets are appropriately classified, protected, retained, monitored, shared, and disposed of in accordance with applicable laws, regulations, contractual obligations, organizational policies, and business requirements.

- **Data Ownership Responsibilities:** Information ownership responsibilities include, but are not limited to:
  - Data classification and categorization
  - Access authorization and approval
  - Retention schedule assignment and review
  - Regulatory and contractual compliance
  - Data quality and integrity oversight
  - Secure disposal authorization
  - Legal hold coordination
  - Third-party sharing and disclosure approvals
  - Customer offboarding requirements
  - Privacy and security control validation
  - Risk management participation
  - Audit and compliance support
- **Clinical Data Owner:** Responsible for the governance, protection, retention, and disposition of clinical and healthcare-related information assets.
  - Clinical Records
  - Treatment Plans
  - Progress Notes
  - SOAP Notes
  - Care Plans
  - Assessments
  - Care Coordination Records
  - Behavioral Health Documentation
  - Wellness Documentation
  - Clinical Communications
  - **Responsibilities**
    - Approve clinical record retention schedules.

        - Validate legal, regulatory, payer, and contractual retention requirements.
        - Review and authorize disposition requests.
        - Support continuity-of-care obligations.
        - Ensure compliance with applicable healthcare regulations.
        - Participate in clinical information governance reviews.
        - Support audit, compliance, and regulatory activities.
- **Security Data Owner:** Responsible for the governance and protection of cybersecurity, audit, monitoring, and security operations information.
    - Audit Logs
    - Security Logs
    - Authentication Records
    - SIEM Events
    - Vulnerability Assessments
    - Penetration Test Reports
    - Security Incident Records
    - Threat Intelligence Data
    - Compliance Monitoring Records
    - **Responsibilities**
        - Maintain security record retention schedules.
        - Approve secure disposal activities.
        - Support forensic investigations and incident response activities.
        - Validate security logging and monitoring requirements.
        - Ensure compliance with applicable security standards and regulatory requirements.
        - Participate in risk assessments and security audits.
- **Privacy Data Owner:** Responsible for privacy governance, individual rights management, consent management, and privacy compliance activities.
    - Consent Records
    - Authorization Records
    - Disclosure Logs
    - Privacy Requests
    - GDPR Records
    - CCPA/CPRA Records
    - Individual Rights Requests
    - Privacy Assessments
    - **Responsibilities**
        - Validate privacy-related retention requirements.
        - Oversee privacy request processing.
        - Approve privacy-related deletion activities.

        - Monitor privacy compliance obligations.
        - Support regulatory inquiries and audits.
        - Ensure compliance with applicable privacy laws and regulations.
- **AI Governance Data Owner:** Responsible for governance, oversight, accountability, and lifecycle management of artificial intelligence systems and associated governance records.
    - AI Inventories
    - AI Risk Assessments
    - AI Governance Documentation
    - Human Review Records
    - AI Audit Logs
    - AI Validation Reports
    - AI Training Authorizations
    - Bias Assessments
    - AI Incident Reports
    - **Responsibilities**
        - Review AI retention schedules and governance requirements.
        - Approve AI-related disposition and destruction activities.
        - Monitor compliance with AI governance requirements.
        - Oversee human-in-the-loop validation processes.
        - Review AI risk assessments and monitoring activities.
        - Support responsible AI governance, transparency, accountability, and compliance initiatives.

3.4 Retention Schedule Governance

Policy: Cognera Health shall establish, maintain, and periodically review a documented enterprise records retention and information lifecycle management program that defines retention requirements, archival standards, legal hold procedures, disposition requirements, and secure destruction methodologies for all information assets.

Retention schedules shall be designed to support regulatory compliance, privacy obligations, information governance, operational requirements, legal preservation needs, business continuity objectives, and risk management activities.

The retention governance program shall support applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Documentation Requirements (45 CFR §164.316(b)(2))
- HIPAA Accounting of Disclosures (45 CFR §164.528)
- HITECH Act

- GDPR Article 5 (Storage Limitation)
- GDPR Article 17 (Right to Erasure)
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- Contractual, legal, regulatory, and business requirements

Procedures

- **Retention Schedule Management:** Cognera Health shall maintain documented retention schedules that identify:
  - Information categories
  - Data owners
  - Applicable regulations
  - Minimum retention periods
  - Archival requirements
  - Legal hold requirements
  - Destruction requirements
  - Secure disposal methodologies
- **Periodic Retention Reviews:** Retention schedules shall be reviewed and updated:
  - Annually
  - Following significant regulatory or legal changes
  - Following material contractual changes
  - Following audit findings or compliance reviews
  - Following mergers, acquisitions, divestitures, or organizational restructuring
  - Following significant operational, technology, or business changes
- **Retention Schedule Approval**: Retention schedules and material modifications shall be reviewed and approved by:
  - Privacy Officer
  - Compliance Officer
  - Legal Counsel
  - Data Governance Committee
  - Where applicable, additional review may be required from Security, Clinical, Compliance, or Executive Leadership.

3.5 Data Minimization and Information Management Principles

Policy: Cognera Health shall collect, create, process, access, use, retain, disclose, and share only the minimum amount of information necessary to support authorized business, clinical, operational, security, contractual, legal, regulatory, and compliance requirements.

Data minimization practices are intended to reduce privacy risk, limit unnecessary exposure of sensitive information, improve information governance, and support compliance with applicable healthcare, privacy, and security requirements.

This policy supports:

- HIPAA Minimum Necessary Standard (45 CFR §164.502(b))
- HIPAA Privacy Rule
- GDPR Article 5(1)(c) (Data Minimization)
- ISO/IEC 27701
- HITRUST Common Security Framework (CSF)
- Industry-recognized privacy and information governance best practices

Procedures

Collection Controls: Cognera Health shall collect only information reasonably necessary to:

- Deliver products and services
- Support clinical care and care coordination
- Support authorized healthcare operations
- Fulfill contractual obligations
- Meet regulatory and legal requirements
- Support security, compliance, and operational activities

Access Controls: Access to information shall be limited to authorized individuals with a legitimate business, clinical, operational, security, or regulatory need-to-know.

Retention Controls: Information shall not be retained longer than necessary to satisfy applicable business, legal, regulatory, contractual, clinical, security, audit, or operational requirements.

Disclosure Controls: Information sharing, disclosure, and transmission activities shall be limited to the minimum amount of information necessary to accomplish the authorized purpose.

Disposition Controls: When information is no longer required and no legal, regulatory, contractual, clinical, or operational preservation requirements exist, the information shall be dispositioned in accordance with approved retention schedules and secure disposal requirements.

Disposition activities may include:

- Secure deletion
- Secure destruction
- De-identification
- Anonymization
- Archival disposition
- Final records disposal

All disposition activities shall be documented, validated, and performed using approved procedures and controls.

4. Data Retention Policies

4.1 General Data Retention Policy

Policy: Cognera Health shall retain information only for as long as necessary to fulfill legitimate business, clinical, operational, legal, contractual, regulatory, privacy, security, audit, risk management, continuity-of-care, and compliance requirements.

Information retention periods shall be based on applicable laws, regulations, contractual obligations, healthcare recordkeeping requirements, industry standards, operational needs, litigation preservation requirements, and organizational risk considerations.

Retention schedules shall support compliance with:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH Act
- GDPR Article 5 (Storage Limitation)
- GDPR Article 17 (Right to Erasure)
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- Applicable state healthcare record retention requirements
- Customer contractual requirements

Retention Objectives: Information may be retained to:

- Deliver and support products and services
- Maintain continuity of care and clinical history
- Support patient, provider, and organizational needs
- Meet regulatory and legal obligations
- Fulfill contractual commitments
- Support investigations, audits, and compliance activities
- Defend legal claims and preserve evidence
- Support cybersecurity monitoring and incident investigations
- Maintain business continuity and disaster recovery capabilities
- Preserve historical records and operational intelligence

- Support authorized analytics, reporting, and quality improvement activities

4.2 Clinical Record Retention

Policy: Cognera Health shall retain clinical, behavioral health, wellness, and care coordination records in accordance with applicable federal laws, state laws, healthcare regulations, accreditation requirements, payer requirements, contractual obligations, and customer record retention policies.

Clinical records constitute part of the designated record set and shall be protected, retained, archived, and disposed of in accordance with approved retention schedules and continuity-of-care requirements.

Covered Clinical Records: Clinical records include healthcare, behavioral health, wellness, care management, care coordination, operational, and treatment-related documentation generated, collected, maintained, or processed through Cognera Health platforms and services in support of care delivery, clinical decision-making, treatment planning, continuity of care, regulatory compliance, quality improvement, and outcome measurement.

Clinical records may include, but are not limited to:

- Clinical Documentation and Clinical Notes
- Progress Notes and Encounter Documentation
- SOAP Notes and Session Documentation
- Treatment Plans, Care Plans, and Recovery Plans
- Behavioral Health, Mental Health, and Wellness Records
- Intake, Assessment, and Evaluation Documentation
- Care Coordination and Care Management Records
- Case Management and Referral Documentation
- Clinical Summaries and Treatment Summaries
- Clinical Recommendations and Clinical Decision Support Records
- Intervention Documentation and Therapeutic Activity Records
- Crisis Intervention, Crisis Monitoring, and Crisis Management Documentation
- Medication Management and Medication Monitoring Records
- Patient-Reported Outcomes and Provider-Reported Outcomes
- Measurement-Based Care Records and Assessment Results
- Outcome Tracking, Progress Monitoring, and Longitudinal Care Records
- Engagement, Adherence, and Follow-Up Documentation
- Communication Records Incorporated into the Clinical Record
- Voice-to-Text Transcriptions Incorporated into the Clinical Record
- Care Team Collaboration and Multidisciplinary Care Documentation

- Clinical Intelligence, Risk Assessment, and Care Planning Records
- Organization-Specific Clinical Documentation Requirements
- Other healthcare, behavioral health, wellness, operational, or treatment-related records maintained as part of the designated clinical record set or customer-defined record systems.

Retention Period: Seven (7) years following the last clinical activity, encounter, service, or documented interaction unless a longer retention period is required by:

- State law
- Federal law
- Contractual obligations
- Payer requirements
- Accreditation standards
- Litigation holds
- Regulatory investigations
- Customer requirements

Archival Requirements: After active use, clinical records may be archived in secure storage environments while maintaining:

- Confidentiality
- Integrity
- Availability
- Auditability
- Accessibility for authorized purposes

4.3 Assessment Retention

Policy: Assessment instruments, screening tools, outcome measures, questionnaires, and measurement-based care records shall be retained as part of the designated clinical record set and governed by clinical record retention requirements.

Covered Assessments and Measurement Instruments

Assessment records include standardized clinical assessments, behavioral health screening tools, wellness evaluations, outcome measures, risk assessments, symptom monitoring instruments, measurement-based care tools, and other validated or organization-approved assessment instruments utilized to support screening, evaluation, treatment planning, progress monitoring, clinical decision support, outcome measurement, quality improvement, and continuous care delivery.

Examples include, but are not limited to:

- Depression Screening and Outcome Measures (e.g., PHQ-9, BDI)

- Anxiety Screening and Outcome Measures (e.g., GAD-7, BAI)
- Behavioral Health and Mental Health Assessments
- Outcome Measurement Instruments (e.g., OQ-45.2)
- Suicide Risk and Crisis Screening Instruments (e.g., C-SSRS)
- Attention, Cognitive, and Neurobehavioral Assessments (e.g., ASRS)
- Substance Use and Addiction Screening Instruments (e.g., AUDIT, DAST)
- Trauma and PTSD Assessments (e.g., PCL-5)
- Wellness, Well-Being, and Quality-of-Life Assessments (e.g., WHO-5)
- Recovery, Resilience, and Functional Status Assessments
- Clinical Intake Assessments
- Risk Stratification and Risk Screening Instruments
- Measurement-Based Care Assessments
- Patient-Reported Outcome Measures (PROMs)
- Provider-Reported Outcome Measures
- Engagement and Adherence Assessments
- Population Health and Care Management Assessments
- Organization-Specific and Customer-Defined Assessments
- Custom Clinical, Behavioral Health, Wellness, and Operational Assessments
- Other validated or approved assessment instruments utilized within Cognera Health platforms and services.
- Risk Screening Instruments

Retention Period: Seven (7) years or longer where required by law, regulation, contract, accreditation requirements, payer requirements, or customer policies.

Assessment Governance: Assessment records shall:

- Remain associated with the clinical record
- Be available for longitudinal outcome analysis
- Support measurement-based care initiatives
- Support audit and quality improvement activities

4.4 Messaging and Communication Records

Policy: Electronic communications supporting care delivery, coordination, engagement, treatment planning, provider collaboration, operational workflows, and healthcare services shall be retained as part of the applicable clinical or operational record.

Covered Communications

- Examples:
  - Secure Messaging

- Provider-to-Provider Communications
- Provider-to-Individual Communications
- Care Team Communications
- Care Coordination Messages
- Clinical Collaboration Records
- Workflow Communications
- Intervention Communications
- Follow-Up Communications
- Engagement Communications

Retention Period: Seven (7) years or longer where required by applicable retention requirements.

Communication records shall maintain:

- Message content
- Metadata
- Sender information
- Recipient information
- Delivery records
- Audit records where applicable.

4.5 Authorization and Consent Records

Policy: Authorization, consent, acknowledgment, and permission records shall be retained in accordance with HIPAA, HITECH, privacy regulations, contractual requirements, and organizational governance requirements.

References: 45 CFR §164.508 & 45 CFR §164.316(b)(2)

Covered Records

Examples include:

- HIPAA Authorizations
- Release of Information Authorizations
- Disclosure Authorizations
- Marketing Authorizations
- Research Authorizations
- Voice Recording Consents
- Telehealth Consents
- AI Processing Authorizations
- Data Sharing Consents
- Revocation Requests

Retention Period: Six (6) years from creation date or last effective date, whichever is later

Authorization records shall:

- Remain auditable
- Support regulatory reviews
- Support disclosure tracking
- Maintain version history where applicable

4.6 Disclosure Records

Policy: Cognera Health shall maintain records of disclosures of PHI and regulated information as required by HIPAA and applicable privacy regulations.

References: 45 CFR §164.528

Covered Records

- Accounting of Disclosures
- Disclosure Logs
- External Sharing Records
- Release of Information Records
- Authorized Disclosure Records
- Regulatory Disclosure Records

Retention Period: Six (6) years

Disclosure records shall include:

- Date of disclosure
- Recipient
- Purpose
- Information disclosed
- Authorization references where applicable
- Supporting documentation

4.7 Security Records Retention

Policy: Security records shall be retained to support cybersecurity operations, investigations, forensic analysis, incident response, compliance activities, audits, and regulatory requirements.

Security Retention Schedule

Record Type	Minimum Retention

Audit Logs	6 Years
Authentication Logs	6 Years
Access Logs	6 Years
Security Event Logs	6 Years
SIEM Records	6 Years
Security Incident Records	6 Years
Breach Investigation Records	6 Years
Vulnerability Assessments	6 Years
Vulnerability Scans	6 Years
Penetration Test Reports	6 Years
Risk Assessments	6 Years
Security Monitoring Reports	6 Years
Threat Intelligence Records	6 Years
Compliance Monitoring Records	6 Years

Security records shall support:

- Incident investigations
- Forensic analysis
- Regulatory reviews
- Internal audits
- External audits
- Compliance reporting

4.8 HIPAA, Compliance, and Governance Records

Policy: Cognera Health shall maintain compliance, governance, training, audit, and regulatory records necessary to demonstrate compliance with HIPAA, HITECH, privacy laws, security standards, and organizational governance requirements.

References: 45 CFR §164.316(b)(2) & HITECH Act

Retention Schedule

Record Type	Minimum Retention
Policies	6 Years
Procedures	6 Years
HIPAA Training Records	6 Years
Compliance Training Records	6 Years
Business Associate Agreements (BAAs)	6 Years After Termination
Compliance Reviews	6 Years
Internal Audit Reports	6 Years

External Audit Reports	6 Years
OCR Correspondence	6 Years
Regulatory Inquiry Records	6 Years
Corrective Action Plans	6 Years
Governance Committee Records	6 Years
Risk Management Reviews	6 Years
AI Governance Records	6 Years

Compliance records shall:

- Be maintained in secure repositories
- Support regulatory inspections
- Support audit readiness
- Support compliance validation
- Be accessible to authorized personnel
- Be retained in accordance with applicable legal and regulatory requirements

5. Data Subject Rights Management

5.1 Privacy Rights and Individual Rights Management Policy

Policy: Cognera Health is committed to protecting individual privacy rights and supporting applicable data subject, consumer, patient, customer, and user rights in accordance with applicable privacy laws, healthcare regulations, contractual obligations, and organizational governance requirements.

Where applicable, Cognera Health shall establish procedures, controls, and governance processes to facilitate the identification, validation, processing, documentation, and fulfillment of privacy rights requests while balancing regulatory, legal, security, healthcare, continuity-of-care, and contractual obligations.

This policy supports applicable requirements arising from:

- General Data Protection Regulation (GDPR) Articles 12–23
- UK General Data Protection Regulation (UK GDPR)
- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Applicable U.S. State Privacy Laws
- Consumer Health Privacy Laws
- Applicable healthcare privacy and information governance requirements
- Customer contractual privacy obligations

- **Privacy Rights Governance Objectives**
  - Cognera Health shall:
  - Promote transparency regarding personal data processing activities.
  - Support lawful and timely responses to privacy rights requests.
  - Protect individual privacy and consumer rights.
  - Maintain appropriate safeguards against unauthorized disclosures.
  - Balance privacy rights with healthcare, regulatory, legal, contractual, security, and operational requirements.
  - Maintain documentation and audit trails supporting privacy rights compliance.

- **Supported Individual Privacy Rights**
  - **Right of Access**
    - **Reference:** GDPR Article 15 & Applicable State Privacy Laws
    - **Description:** Individuals may request information regarding:
      - Personal data processed by Cognera Health
      - Categories of personal information collected
      - Purposes of processing
      - Categories of recipients
      - Sources of personal information
      - Applicable retention periods
      - Data sharing and disclosure activities
      - Applicable privacy rights
    - **Requirements:** Cognera Health shall provide information in a secure, commonly used, and accessible format where legally required and operationally feasible.
  - **Right to Rectification**
    - **Reference:** GDPR Article 16
    - **Description:** Individuals may request correction of inaccurate, incomplete, outdated, or misleading personal information maintained by Cognera Health.
    - **Requirements:** Correction requests shall be reviewed, validated, documented, and processed in accordance with applicable legal, healthcare, operational, and contractual requirements.
  - **Right to Erasure (Right to be Forgotten)**
    - **Reference:** GDPR Article 17
    - **Description:** Individuals may request deletion of personal information where applicable legal grounds exist.
    - **Limitations:** Deletion requests may be limited or denied where information must be retained for:
      - Healthcare record retention requirements
      - HIPAA obligations

    - Regulatory requirements
    - Legal preservation requirements
    - Litigation holds
    - Security investigations
    - Fraud prevention activities
    - Contractual obligations
    - Continuity-of-care requirements
- **Right to Restrict Processing**
    - **Reference:** GDPR Article 18
    - **Description:** Individuals may request restriction of processing activities under circumstances permitted by applicable law.
    - Restrictions may apply to:
        - Data processing activities
        - Data sharing activities
        - Analytics activities
        - Marketing activities
        - Certain operational processing activities
- **Right to Data Portability**
    - **Reference:** GDPR Article 20
    - **Description:** Individuals may request that personal information be provided in a structured, commonly used, and machine-readable format where legally applicable. Where technically feasible and legally permissible, data may be transmitted to another authorized organization at the individual's direction.
- **Right to Object**
    - **Reference:** GDPR Article 21
    - **Description:** Individuals may object to certain processing activities where applicable legal rights exist.
    - Objections may relate to:
        - Direct marketing
        - Certain analytics activities
        - Profiling activities
        - Processing based upon legitimate interests
        - Requests shall be reviewed in accordance with applicable legal requirements.
- **Right to Withdraw Consent**
    - **Description:** Where processing is based on consent, individuals may withdraw consent at any time, subject to legal, healthcare, contractual, and operational limitations. Withdrawal of consent shall not affect processing that occurred prior to withdrawal.

- **California Consumer Privacy Rights**
  - **Applicable Rights:** Where applicable under CCPA and CPRA, California residents may exercise the following rights:
    - Right to Know
    - Right to Access
    - Right to Delete
    - Right to Correct
    - Right to Limit Use of Sensitive Personal Information
    - Right to Opt-Out of Certain Data Sharing Activities
    - Right to non-discrimination
    - Right to Equal Service and Pricing

  Cognera Health shall not discriminate against individuals who exercise lawful privacy rights.

- **Request Processing and Verification Procedures**
  - **Policy:** Prior to disclosing, modifying, restricting, deleting, exporting, or otherwise processing personal information in response to a privacy rights request, Cognera Health shall take reasonable measures to verify the identity and authority of the requestor.
  - **Identity Verification:** Verification procedures may include:
    - Account authentication
    - Multi-factor authentication
    - Identity validation
    - Customer administrator verification
    - Authorized representative verification
    - Documentation review
    - Additional validation procedures where appropriate
  - **Authorization Validation:** Where requests are submitted by third parties, Cognera Health shall verify:
    - Legal authority
    - Written authorization
    - Applicable consent requirements
    - Representative authority
  - **Fraud Prevention Review:** Privacy rights requests may be reviewed for:
    - Fraud indicators
    - Identity theft concerns
    - Unauthorized access attempts
    - Security risks
    - Regulatory concerns
  - **Request Response Timeframes:** Cognera Health shall make reasonable efforts to process privacy rights requests within applicable legal timeframes.

Request Type	Standard Response Time
Access Request	30 Days
Correction Request	30 Days
Data Portability Request	30 Days
Deletion Request	30 Days
Restriction Request	30 Days
Objection Request	30 Days
Consumer Privacy Request	30 Days

Where permitted by applicable law, response periods may be extended when:

- Requests are unusually complex
- Additional verification is required
- Multiple requests are received
- Legal review is necessary
- Operational constraints exist

Individuals shall be notified of any approved extensions and the reason for the extension.

- **Documentation and Audit Requirements:** Cognera Health shall maintain records of:
  - Privacy rights requests
  - Verification activities
  - Response actions
  - Extension notices
  - Denial determinations
  - Regulatory correspondence
  - Supporting documentation

Privacy rights records shall be retained in accordance with approved retention schedules and applicable regulatory requirements.

- **Compliance Monitoring:** Privacy rights management activities shall be periodically reviewed through:
  - Internal compliance reviews
  - Privacy audits
  - Regulatory assessments
  - Risk assessments
  - Governance reviews
  - Corrective action programs

Results shall be reported to appropriate governance, compliance, privacy, and leadership stakeholders to support continuous improvement and regulatory readiness.

6. Data Deletion and Information Disposition Policies

6.1 General Data Deletion and Information Disposition Policy

Policy: Cognera Health shall implement and maintain documented, auditable, and defensible processes governing the deletion, destruction, de-identification, anonymization, archival disposition, and final disposition of information assets throughout their lifecycle.

Information shall only be deleted, destroyed, de-identified, anonymized, or otherwise dispositioned after applicable retention requirements have been satisfied and provided that no legal, regulatory, contractual, clinical, operational, security, audit, investigative, or preservation obligations require continued retention.

All deletion and disposition activities shall be performed in a manner that protects confidentiality, integrity, availability, privacy, security, continuity-of-care obligations, regulatory compliance, and organizational governance requirements.

- **Regulatory and Standards Alignment**

Deletion and disposition activities shall support applicable requirements arising from:

  - HIPAA Privacy Rule
  - HIPAA Security Rule
  - HITECH Act
  - HIPAA Documentation Requirements (45 CFR §164.316)
  - GDPR Article 5 (Storage Limitation)
  - GDPR Article 17 (Right to Erasure)
  - GDPR Article 25 (Privacy by Design)
  - CCPA
  - CPRA
  - HITRUST Common Security Framework (CSF)
  - ISO/IEC 27001
  - ISO/IEC 27701
  - NIST SP 800-88 Rev.1 (Media Sanitization)
  - Applicable state privacy laws
  - Applicable healthcare record retention laws
  - Contractual obligations

- **Deletion Objectives**

Cognera Health shall perform information disposition activities to:

- Reduce privacy and security risk
- Support regulatory compliance
- Eliminate unnecessary data retention
- Support data minimization principles
- Reduce organizational liability
- Protect individual privacy rights
- Support contractual requirements
- Improve information governance maturity
- Maintain accurate and defensible records management practices

6.2 Authorized Deletion and Disposition Triggers

Policy: Deletion, destruction, de-identification, anonymization, or other disposition activities may occur only upon authorized triggering events and after completion of required validation and approval activities.

- **Authorized Deletion Triggers**

Deletion activities may be initiated following:

- Expiration of approved retention periods
- Verified privacy rights requests
- Customer-approved deletion requests
- Contract termination or customer offboarding
- Data minimization initiatives
- System decommissioning or replacement
- Data migration projects
- Infrastructure retirement activities
- Vendor termination activities
- Regulatory requirements
- Legal authorization
- Approved records disposition schedules
- Security remediation activities
- Compliance-directed cleanup activities

- **Prohibited Deletion Events**

Information shall not be deleted when:

- Active legal holds exist
- Litigation is pending

- Regulatory investigations are active
- Security investigations are ongoing
- Audit requirements remain outstanding
- Contractual retention obligations remain active
- Continuity-of-care requirements require preservation
- Healthcare record retention requirements remain active

6.3 Data Deletion Procedures

Policy: Cognera Health shall implement documented, repeatable, controlled, and auditable deletion procedures to ensure information is removed, destroyed, anonymized, or de-identified in a secure, verifiable, and compliant manner.

Deletion activities shall be governed through approved procedures, validation requirements, audit controls, monitoring activities, and governance oversight.

- **Regulatory References**
  - HIPAA Privacy Rule (45 CFR Part 164)
  - HIPAA Security Rule (45 CFR §164.308(a)(1))
  - HIPAA Security Rule (45 CFR §164.312)
  - HITECH Act
  - GDPR Article 17
  - GDPR Article 25
  - CCPA / CPRA
  - HITRUST CSF
  - ISO/IEC 27001
  - ISO/IEC 27701
  - NIST SP 800-88 Rev.1

- **Deletion Authorization Procedures**

Prior to any deletion activity, the following validation activities shall be completed:

  - Verify applicable retention periods have expired.
  - Verify information classification.
  - Verify ownership and stewardship approvals.
  - Verify legal hold status.
  - Verify litigation preservation requirements.
  - Verify regulatory preservation requirements.
  - Verify contractual obligations.
  - Verify customer requirements.
  - Verify continuity-of-care obligations.

- Verify security investigation requirements.
- Document required approvals.
- Record deletion authorization activities.

- **Deletion Execution Procedures**

Deletion activities may include:

- Application-level deletion
- Database record deletion
- File deletion
- Secure overwrite
- Cryptographic erasure
- Media sanitization
- Backup expiration processing
- Secure destruction
- De-identification
- Anonymization

Deletion methods shall be appropriate to:

- Information classification
- Risk level
- Regulatory requirements
- Media type
- Technology platform

- **Deletion Verification Procedures**

All deletion activities shall undergo verification to confirm successful completion.

Verification activities may include:

- Automated deletion validation
- Application validation testing
- Audit log review
- Security review
- Compliance review
- Backup lifecycle review
- Destruction certificate review
- Data inventory validation
- Sampling and verification testing

- **Deletion Documentation and Evidence**

Cognera Health shall maintain evidence supporting all approved deletion and destruction activities.

Deletion evidence may include:

  - Request Identifier
  - Approval Records
  - Data Owner Authorization
  - Date and Time of Deletion
  - System or Repository Affected
  - Information Classification
  - Information Category
  - Deletion Method Used
  - Individual Performing Activity
  - Verification Results
  - Supporting Audit Records

- **Retention of Deletion Evidence**

Deletion records shall be retained for: Minimum Six (6) Years unless a longer retention period is required by law, regulation, contract, or organizational policy.

6.4 Customer and Individual Deletion Requests

Policy: Cognera Health shall provide reasonable mechanisms allowing authorized individuals, customers, organizations, Covered Entities, and authorized representatives to request deletion of information where legally permissible.

Regulatory References

- GDPR Article 17
- GDPR Article 12
- GDPR Article 19
- CCPA §1798.105
- CPRA
- Applicable state privacy laws

Request Submission Channels

Deletion requests may be submitted through:

- Privacy Portal

- Customer Administrator
- Covered Entity Administrator
- Privacy Officer
- Compliance Officer
- Authorized Representative
- Customer Support
- Written Privacy Requests

Identity Verification Requirements

Prior to processing any deletion request, Cognera Health shall perform reasonable verification activities.

Verification procedures may include:

- Account verification
- Identity verification
- Multi-factor authentication
- Authorized representative validation
- Covered Entity authorization verification
- Documentation review
- Additional risk-based validation procedures

Authorization Validation

Where requests originate from third parties, Cognera Health shall verify:

- Legal authority
- Written authorization
- Organizational authority
- Applicable consent requirements
- Contractual authorization

Fraud Prevention and Security Review

Deletion requests may undergo review for:

- Identity theft indicators
- Fraud indicators
- Unauthorized access attempts
- Security concerns

- Regulatory risks
- Data ownership conflicts

Completion Timeframes

Approved deletion requests shall be processed within: Thirty (30) Calendar Days unless otherwise required by law or permitted through approved extensions.

Where extensions are permitted, requestors shall be notified of:

- Extension reason
- Revised timeline
- Applicable rights

6.5 Exceptions and Preservation Requirements

Policy: Certain information may be exempt from deletion where legal, regulatory, contractual, healthcare, operational, audit, security, or business requirements necessitate continued retention.

Deletion Exceptions

Deletion requests may be denied, restricted, deferred, or partially fulfilled when:

- HIPAA retention requirements apply.
- Healthcare record retention laws apply.
- Active legal holds exist.
- Pending litigation exists.
- Regulatory investigations are active.
- OCR investigations are active.
- Security investigations are ongoing.
- Fraud investigations are ongoing.
- Contractual retention obligations exist.
- Business continuity requirements exist.
- Continuity-of-care requirements exist.
- Audit requirements remain outstanding.
- Information is required to establish, exercise, or defend legal claims.
- Applicable laws require preservation.

Documentation Requirements

All deletion denials, exceptions, restrictions, and preservation determinations shall be documented and retained in accordance with approved retention schedules.

Supporting documentation shall include:

- Reason for denial
- Applicable legal basis
- Preservation authority
- Review date
- Approval records
- Supporting evidence
- Communication records

Governance Oversight

Deletion exception reviews where appropriate may involve:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Data Governance Committee
- Security Leadership
- Customer Representatives.

7. HIPAA, HITECH, and Regulatory Record Retention Requirements

7.1 Regulatory Record Retention Policy

Policy: Cognera Health shall establish, maintain, protect, and retain records required to demonstrate compliance with applicable healthcare regulations, privacy laws, cybersecurity requirements, contractual obligations, and organizational governance standards.

Compliance, governance, privacy, security, audit, risk management, training, and operational records shall be retained in accordance with applicable regulatory requirements, including HIPAA, HITECH, privacy regulations, industry standards, contractual commitments, and organizational retention schedules.

Retention requirements are intended to support:

- Regulatory compliance
- Audit readiness
- Legal defensibility
- Risk management
- Incident investigations
- Compliance monitoring

- Privacy and security oversight
- Organizational governance
- Customer and contractual obligations
- Continuous improvement initiatives

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Breach Notification Rule
- HITECH Act
- 45 CFR §164.316(b)(2)
- 45 CFR §164.528
- 45 CFR §164.508
- GDPR
- UK GDPR
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- NIST Cybersecurity Framework
- Applicable healthcare regulations and contractual requirements

7.2 HIPAA Documentation Retention Requirements

Policy: Cognera Health shall retain documentation required to demonstrate implementation, operation, monitoring, maintenance, and enforcement of privacy, security, compliance, governance, and risk management controls required under HIPAA.

Required documentation shall be maintained in secure, auditable, and retrievable formats capable of supporting regulatory reviews, investigations, compliance assessments, and audit activities.

Reference: 45 CFR §164.316(b)(2)

Covered Documentation

HIPAA documentation may include, but is not limited to:

- Policies
- Procedures
- Standards
- Guidelines
- Risk Assessments

- Risk Treatment Plans
- Security Reviews
- Compliance Reviews
- Internal Audit Reports
- External Audit Reports
- Incident Reports
- Breach Investigations
- Workforce Training Records
- Access Reviews
- Vendor Assessments
- Business Associate Agreements (BAAs)
- Privacy Reviews
- Security Monitoring Reports
- Governance Committee Records
- Corrective Action Plans
- Regulatory Correspondence
- Documentation Supporting HIPAA Compliance Activities

Retention Requirement: Minimum Retention Period is Six (6) Years from the date of creation or the date when the document was last in effect, whichever is later.
Requirements

HIPAA compliance documentation shall:

- Be maintained in secure repositories.
- Be protected from unauthorized access, modification, or destruction.
- Be available for authorized audit, compliance, regulatory, legal, and operational purposes.
- Support historical compliance validation and regulatory inquiries.

7.3 Accounting of Disclosures Retention Requirements

Policy: Cognera Health shall maintain records supporting the accounting of disclosures of Protected Health Information (PHI) where required by HIPAA and applicable contractual obligations.

Reference: 45 CFR §164.528

Covered Records
Examples include:

- Disclosure Logs
- Disclosure Reports

- Release of Information Records
- Third-Party Disclosure Records
- Regulatory Disclosure Records
- Authorized Disclosure Documentation
- Disclosure Tracking Records

Retention Requirement: Minimum Retention Period is Six (6) Years disclosure records shall include, where applicable:

- Date of disclosure
- Recipient of disclosure
- Purpose of disclosure
- Information disclosed
- Authorization references
- Supporting documentation
- Applicable regulatory or contractual justification

7.4 Authorization and Consent Record Retention Requirements

Policy: Cognera Health shall maintain documentation supporting authorizations, permissions, acknowledgements, and consents involving the use, disclosure, sharing, processing, or retention of Protected Health Information and regulated personal information.

Reference: 45 CFR §164.508

Covered Records
Examples include:

- HIPAA Authorizations
- Release of Information Authorizations
- Research Authorizations
- Voice Recording Consents
- AI Processing Authorizations
- Data Sharing Consents
- Marketing Authorizations
- Telehealth Consents
- Revocation Requests
- Consent Withdrawal Records

Retention Requirement: Minimum Retention Period is Six (6) Years from the date of creation or last effective date, whichever is later.

Authorization records shall:

- Remain auditable.
- Maintain version history where applicable.
- Support regulatory review and compliance activities.
- Support disclosure validation and authorization verification processes.

7.5 HITECH Documentation and Compliance Record Retention

Policy: Cognera Health shall retain records required to demonstrate compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act and related privacy, security, breach notification, and enforcement requirements.

Covered Documentation

HITECH-related records may include:

- Breach Notifications
- Security Incident Investigations
- Breach Risk Assessments
- Regulatory Reporting Documentation
- HHS Correspondence
- OCR Correspondence
- Corrective Action Plans
- Compliance Reviews
- Security Reviews
- Investigation Reports
- Risk Assessments
- Vendor Compliance Reviews
- Enforcement Documentation
- Audit Response Documentation
- Breach Response Activities
- Remediation Plans

Retention Requirement: Minimum Retention Period is Six (6) Years unless a longer retention period is required by law, contract, litigation hold, regulatory inquiry, or organizational policy.

Requirements

HITECH-related documentation shall support:

- Regulatory reviews
- OCR investigations

- HHS inquiries
- Breach response validation
- Audit readiness
- Corrective action tracking
- Compliance monitoring
- Organizational governance activities

7.6 Regulatory Correspondence and Enforcement Documentation

Policy: Cognera Health shall maintain records of communications, inquiries, investigations, enforcement actions, audit activities, and regulatory interactions involving healthcare, privacy, security, and compliance obligations.

Covered Records

Examples include:

- OCR Communications
- HHS Communications
- Regulatory Requests
- Audit Notifications
- Investigation Correspondence
- Compliance Certifications
- Regulatory Responses
- Enforcement Documentation
- Regulatory Findings
- Remediation Activities

Retention Requirement: Minimum Retention Period is Six (6) Years or longer where required by law, settlement agreement, corrective action plan, litigation hold, or regulatory directive.

7.7 Governance, Audit, and Compliance Monitoring Records

Policy: Cognera Health shall maintain governance and compliance records necessary to demonstrate ongoing oversight, monitoring, accountability, and effectiveness of the compliance governance program.

Covered Records

Examples include:

- Governance Committee Minutes
- Compliance Dashboard Reports
- Compliance Metrics
- Audit Findings

- Corrective Actions
- Risk Management Reviews
- Policy Reviews
- Training Effectiveness Reviews
- Compliance Program Assessments
- Annual Governance Reviews

Retention Requirement: Minimum Retention Period is Six (6) Years

Requirements

Governance records shall support:

- Executive oversight
- Regulatory readiness
- Continuous improvement
- Compliance program effectiveness
- Internal and external audit activities
- Enterprise risk management activities

8. Artificial Intelligence, Analytics, and Machine Learning Data Retention Requirements

8.1 Artificial Intelligence Governance and Documentation Retention Policy

Policy: Cognera Health shall establish and maintain comprehensive records, documentation, audit trails, governance artifacts, monitoring activities, and oversight mechanisms supporting the responsible design, development, deployment, operation, monitoring, validation, review, and governance of Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP), Natural Language Understanding (NLU), predictive analytics, clinical decision support, and intelligent automation capabilities utilized within Cognera Health platforms and services.

AI governance documentation shall support transparency, explainability, accountability, auditability, risk management, human oversight, regulatory compliance, model governance, quality assurance, security, privacy protection, and responsible AI practices.

Documentation shall be sufficient to demonstrate that AI-enabled capabilities operate in accordance with applicable laws, regulations, governance requirements, ethical principles, clinical oversight requirements, and organizational policies.

- **Regulatory and Standards Alignment**

This policy supports applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH Act
- 45 CFR §164.308
- 45 CFR §164.312
- 45 CFR §164.502
- 45 CFR §164.508
- GDPR
- UK GDPR
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- NIST Artificial Intelligence Risk Management Framework (AI RMF)
- NIST Cybersecurity Framework
- ISO/IEC 27001
- ISO/IEC 27701
- ISO/IEC 42001 Artificial Intelligence Management Systems (where applicable)
- Applicable healthcare regulatory requirements
- Responsible AI governance principles

- **AI Governance Objectives**

Cognera Health shall maintain records supporting:

- Transparency
- Explainability
- Accountability
- Human-in-the-loop oversight
- Clinical oversight
- Risk management
- Bias monitoring
- Fairness assessments
- Model validation
- Security monitoring
- Privacy protection
- Continuous improvement
- Regulatory readiness
- Audit readiness

- **AI Governance Documentation**

Cognera Health shall maintain documentation including, but not limited to:

AI Governance Records

- AI Governance Policies
- AI Governance Procedures
- AI Governance Reviews
- AI Oversight Committee Records
- Governance Meeting Minutes
- Responsible AI Assessments

AI Inventory Records

- AI Model Inventory
- Model Registry Records
- Model Ownership Records
- Model Purpose Documentation
- Model Architecture Documentation
- Model Lifecycle Documentation

AI Risk and Compliance Records

- AI Risk Assessments
- Bias Assessments
- Fairness Reviews
- Security Assessments
- Privacy Impact Assessments
- Compliance Reviews
- Regulatory Assessments

AI Validation Records

- Validation Reports
- Verification Reports
- Model Testing Results
- Accuracy Reviews
- Performance Evaluations
- Outcome Validation Records

Human Oversight Records

- Human Review Logs
- Human Validation Records
- Human Override Records
- Escalation Reviews
- Clinical Review Records

AI Monitoring Records

- Model Performance Monitoring

- Drift Detection Reports
- Anomaly Detection Reports
- Monitoring Dashboards
- Operational Performance Reviews

AI Incident Records

- AI Incident Reports
- AI Error Reviews
- Model Failure Reviews
- Corrective Action Plans
- Root Cause Analyses

Retention Requirement: Minimum Retention Period is Six (6) Years unless a longer retention period is required by law, regulation, contract, litigation hold, customer requirement, or organizational policy.

8.2 AI Training Data Governance and Retention

Policy: Protected Health Information (PHI), electronic Protected Health Information (ePHI), personally identifiable information, regulated healthcare information, or other sensitive information shall not be used for AI model training, retraining, fine-tuning, validation, benchmarking, or machine learning development activities unless expressly authorized and legally permissible.
References: 45 CFR §164.502, 45 CFR §164.508, HIPAA Privacy Rule, HIPAA Security Rule and HITECH Act

Requirements

Where PHI or regulated information is authorized for AI-related processing:

- Authorization requirements shall be documented.
- Data minimization principles shall be applied.
- Access shall be restricted to authorized personnel.
- Processing activities shall be logged.
- Privacy safeguards shall be implemented.
- Security controls shall be enforced.
- Human oversight shall be maintained.
- Data usage shall be auditable.

AI Training Documentation

Where authorized, Cognera Health shall maintain:

- Authorization Records
- Consent Documentation
- Data Use Agreements

- Training Activity Logs
- Dataset Documentation
- Data Source Documentation
- Data Lineage Records
- Data Quality Assessments
- Training Environment Documentation
- Security Reviews
- Privacy Reviews
- Validation Reports
- Model Release Documentation
- Version Histories
- Model Change Records

Retention Requirement: Minimum Retention Period Six (6) Years from the date of creation, training activity, authorization expiration, or model retirement, whichever is later.

8.3 AI Audit Logging and Activity Monitoring

Policy: Cognera Health shall maintain audit logs, monitoring records, usage records, operational records, and oversight documentation sufficient to support accountability, transparency, forensic investigations, compliance reviews, operational monitoring, and regulatory audits.

AI Audit Records
Examples include:

Model Activity Records

- Model Execution Logs
- Inference Records
- Recommendation Logs
- Prediction Logs
- Classification Logs
- Prompt Processing Records
- Response Generation Records

User Activity Records

- User Review Actions
- Human Validation Activities
- Human Approval Records
- Human Override Decisions
- Escalation Activities
- Feedback Records

Validation Records

- Validation Outcomes
- Accuracy Evaluations
- Clinical Review Outcomes
- Quality Assurance Reviews
- Monitoring Results

Operational Monitoring Records

- Drift Detection Events
- Performance Monitoring Logs
- System Health Records
- Operational Analytics
- Security Monitoring Records

Compliance Monitoring Records

- Compliance Reviews
- Governance Reviews
- Audit Findings
- Corrective Actions
- Regulatory Assessments

Retention Requirement: Minimum Retention Period is Six (6) Years unless a longer retention period is required by law, regulation, customer agreement, litigation hold, regulatory inquiry, or organizational policy.

8.4 AI Model Retirement and Disposition

Policy: Cognera Health shall maintain records supporting the retirement, replacement, decommissioning, archival, and disposition of AI models and related governance artifacts.

Required Records

- Retirement Approvals
- Model Decommissioning Documentation
- Archived Model Records
- Final Validation Reports
- Risk Closure Reviews
- Data Disposition Records
- Security Reviews
- Compliance Reviews
- Governance Approvals

Retention Requirement: Minimum Retention Period is Six (6) Years following model retirement or

decommissioning unless otherwise required by applicable legal, regulatory, contractual, or organizational requirements.

9. Voice-to-Text, Audio, and Transcription Data Retention Requirements

9.1 Voice, Audio, and Speech Processing Governance Policy

Policy: Cognera Health shall establish and maintain administrative, technical, operational, privacy, security, retention, and governance controls governing the collection, processing, storage, transmission, transcription, retention, deletion, and disposition of audio recordings, voice inputs, speech-to-text data, transcriptions, and related metadata that may contain Protected Health Information (PHI), electronic Protected Health Information (ePHI), personal information, consumer health data, or other sensitive information.

Audio recordings, voice interactions, speech-derived content, and transcribed records shall be protected using the same privacy, security, compliance, retention, monitoring, and governance requirements applied to other forms of regulated healthcare and personal information.

Voice-related information shall be governed throughout its lifecycle to support privacy, security, auditability, continuity of care, compliance, operational integrity, and responsible use of voice-enabled technologies.

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Breach Notification Rule
- HITECH Act
- 45 CFR §164.308 Administrative Safeguards
- 45 CFR §164.312 Technical Safeguards
- 45 CFR §164.502 Minimum Necessary Standard
- 45 CFR §164.508 Authorization Requirements
- GDPR
- UK GDPR
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001

- ISO/IEC 27701
- NIST Cybersecurity Framework
- Applicable healthcare privacy and security requirements

9.2 Audio and Voice Data Retention Schedule

Policy: Retention periods for voice recordings, audio files, transcriptions, and related records shall be based on privacy requirements, security requirements, clinical requirements, legal obligations, contractual commitments, customer requirements, and operational needs.

Retention Schedule

Record Type	Minimum Retention Requirement
Raw Audio Recordings	Deleted following successful transcription and validation unless retention is otherwise required
Voice Inputs	Deleted following successful processing unless retention is otherwise required
Audio Access Logs	6 Years
Audio Activity Logs	6 Years
Audio Deletion Logs	6 Years
Voice Consent Records	6 Years
Voice Recording Authorizations	6 Years
Audio Security Reviews	6 Years
Audio Risk Assessments	6 Years
Voice Processing Audit Records	6 Years
Clinical Transcriptions	Same retention period as the associated clinical record
Behavioral Health Transcriptions	Same retention period as the associated clinical record
Wellness Session Transcriptions	Same retention period as the associated clinical record
Voice-to-Text Validation Records	6 Years
Voice Processing Incident Reports	6 Years

9.3 Audio Recording and Voice Processing Requirements

Policy: Audio recordings and voice processing activities involving PHI, ePHI, personal information, or regulated healthcare information shall be subject to documented authorization, monitoring, security controls, retention controls, and audit requirements.

Requirements

Cognera Health shall:

- Treat all voice recordings and audio inputs containing regulated information as sensitive information assets.
- Encrypt audio data at rest and in transit.
- Restrict access to authorized personnel.
- Maintain detailed audit trails.
- Monitor access and usage activity.
- Validate transcription quality and completeness.
- Apply minimum necessary access controls.
- Document retention and deletion activities.
- Perform periodic compliance reviews.

9.4 Audio Deletion and Disposition Procedures

Policy: Raw audio recordings shall not be retained longer than necessary to fulfill authorized business, clinical, operational, legal, security, contractual, or regulatory requirements.

Where audio recordings are utilized solely to generate transcriptions, raw recordings should be removed following successful transcription, validation, and completion of required quality assurance activities.

Deletion Procedures

Prior to deletion, Cognera Health shall:

- Verify successful transcription completion.
- Validate transcription quality and accuracy.
- Verify record integrity and availability.
- Confirm successful storage of the transcription record.
- Verify legal retention requirements.
- Verify contractual retention requirements.
- Verify customer-specific requirements.
- Verify no active legal hold exists.
- Verify no active investigation requires preservation.
- Verify continuity-of-care requirements have been satisfied.
- Following validation:
- Securely delete raw audio files.
- Record deletion activity.
- Update audit records.
- Retain deletion evidence in accordance with approved retention schedules.

9.5 Voice Recording Authorization and Consent Requirements

Policy: Audio recording, voice capture, and speech processing activities involving PHI or regulated information shall be supported by appropriate authorization, consent, legal authority, contractual authority, or other permitted basis for processing.

Documentation Requirements

Cognera Health shall maintain records including:

- Voice Recording Consents
- HIPAA Authorizations
- AI Processing Authorizations
- Voice Processing Acknowledgements
- Consent Revocation Records
- Authorization Updates
- Disclosure Approvals

Retention Requirement: Minimum Retention Period is Six (6) Years or longer where required by law, regulation, contract, customer requirement, or organizational policy.

9.6 Audio Processing Exceptions

Policy: Certain audio recordings may require retention beyond standard deletion schedules when authorized or required by applicable obligations.

Retention Exceptions

Audio recordings may be retained when:

- Contractually required by a customer.
- Legally required by applicable laws or regulations.
- Required for continuity of care.
- Required for quality assurance or compliance review activities.
- Required for security investigations.
- Required for incident investigations.
- Required for litigation preservation.
- Subject to legal hold requirements.
- Explicitly authorized by the individual.
- Required by customer retention policies.
- Required for approved clinical, operational, or regulatory purposes.

Governance Requirements

All exceptions shall:

- Be documented.
- Be approved by authorized personnel.
- Include justification for retention.
- Be reviewed periodically.
- Remain subject to privacy, security, access control, and monitoring requirements.

9.7 Voice-to-Text Monitoring and Compliance Reviews

Policy: Cognera Health shall periodically review voice processing, transcription, retention, deletion, and security controls to ensure compliance with applicable regulatory, contractual, operational, privacy, and security requirements.

Monitoring Activities

Monitoring activities may include:

- Audio access reviews
- Voice processing audits
- Transcription validation reviews
- Consent validation reviews
- Retention schedule reviews
- Deletion verification reviews
- Security assessments
- Privacy compliance reviews
- Vendor assessments
- Risk assessments
- Incident reviews

Retention of Monitoring Records

Monitoring, audit, review, and compliance records related to voice processing activities shall be retained is for Minimum Six (6) Years unless a longer retention period is required by applicable legal, regulatory, contractual, or organizational requirements.

10. Backup, Disaster Recovery, and Archival Data Retention Requirements

10.1 Backup and Disaster Recovery Data Retention Policy

Policy: Cognera Health shall establish, maintain, and periodically review backup, disaster recovery, archival, and data preservation practices designed to support business continuity, disaster

recovery, cybersecurity resilience, operational continuity, regulatory compliance, data availability, system recovery, incident response, and continuity-of-care requirements.

Backup and disaster recovery processes shall ensure the availability, integrity, confidentiality, recoverability, and resilience of information assets while supporting organizational recovery objectives and applicable legal, contractual, security, privacy, and healthcare obligations.

Backup retention schedules shall be based on business requirements, recovery objectives, customer commitments, regulatory requirements, security considerations, operational needs, and contractual obligations.

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Security Rule
- HIPAA Contingency Planning Requirements
- 45 CFR §164.308(a)(7)
- HITECH Act
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53
- NIST SP 800-34 Contingency Planning
- NIST SP 800-88 Media Sanitization
- Applicable contractual obligations
- Business continuity and disaster recovery best practices

Backup and Recovery Objectives

Backup and disaster recovery programs shall support:

- Protection against accidental data loss
- Protection against malicious activity
- Ransomware recovery capabilities
- Disaster recovery readiness
- Operational resilience
- Regulatory compliance
- Continuity of care
- Customer service continuity
- Security incident recovery
- Business continuity objectives

- Data preservation requirements

10.2 Backup and Archival Retention Schedule

Policy: Cognera Health shall maintain documented backup retention schedules that define retention periods for operational backups, recovery archives, disaster recovery copies, and long-term archival data.

Backup Retention Schedule

Backup Type	Minimum Retention Period
Daily Operational Backups	90 Days
Weekly Backup Copies	180 Days
Monthly Backup Archives	12 Months
Quarterly Backup Archives	12 Months
Disaster Recovery Archives	12 Months
Recovery Snapshots	90 Days
Immutable Backup Copies	90 Days or Customer Requirement
Long-Term Archives	Contractual, Regulatory, or Customer Driven
Legal Hold Archives	Until Legal Hold Release
Investigation Preservation Archives	Until Investigation Closure

Retention Extensions

Backup retention periods may be extended where required by:

- Customer agreements
- Regulatory requirements
- Litigation holds
- Security investigations
- Incident response activities
- Audit requirements
- Operational requirements
- Business continuity requirements

10.3 Backup Security Requirements

Policy: All backup, archival, and disaster recovery data shall be protected using appropriate administrative, technical, and organizational safeguards designed to maintain confidentiality, integrity, availability, and recoverability.

Security Requirements

All backup systems shall:

- Utilize AES-256 encryption or equivalent encryption standards for data at rest.
- Utilize secure transmission protocols for data replication and transfer.
- Maintain geographic redundancy across approved locations.
- Maintain logical separation between production and backup environments.
- Implement role-based access controls (RBAC).
- Utilize multi-factor authentication (MFA) for privileged access.
- Maintain immutable backup capabilities where appropriate.
- Support ransomware recovery requirements.
- Be continuously monitored for availability, integrity, and security events.
- Be subject to periodic security reviews and testing.

Backup Access Controls

Access to backup systems shall be restricted to authorized personnel with documented business, operational, security, compliance, or disaster recovery responsibilities.

Access activities shall be:

- Logged
- Audited
- Reviewed periodically
- Monitored for unauthorized activity

10.4 Disaster Recovery and Recovery Testing

Policy: Cognera Health shall periodically test backup and disaster recovery capabilities to validate recoverability, integrity, and effectiveness of recovery procedures.

Procedures

Recovery testing may include:

- Backup restoration testing
- Recovery validation testing
- Disaster recovery simulations
- Business continuity exercises
- Failover testing
- Data integrity verification
- Recovery time objective (RTO) validation
- Recovery point objective (RPO) validation

Documentation

Recovery testing records shall include:

- Test dates
- Systems tested
- Recovery results
- Issues identified
- Corrective actions
- Validation approvals

Retention

Recovery testing documentation shall be retained for is Minimum Six (6) Years

10.5 Backup Monitoring and Compliance Reviews

Policy: Cognera Health shall continuously monitor backup and disaster recovery activities to ensure compliance with retention requirements, security requirements, recovery objectives, and organizational standards.

Monitoring Activities

Monitoring may include:

- Backup completion monitoring
- Replication monitoring
- Recovery monitoring
- Storage utilization monitoring
- Encryption validation
- Access monitoring
- Security event monitoring
- Integrity validation
- Retention schedule compliance reviews
- Disaster recovery readiness assessments

Audit Requirements

Backup activities shall be subject to:

- Internal audits
- Compliance reviews
- Security assessments
- Disaster recovery reviews
- Customer audits where applicable

10.6 Backup Destruction and Media Disposal

Policy: Backup media, archives, snapshots, and disaster recovery copies shall be securely destroyed when retention requirements expire and no legal, regulatory, contractual, operational, or investigative requirements require continued preservation.

Destruction Procedures

Upon expiration of approved retention periods:

- Backup media shall be securely destroyed or sanitized.
- Archived data shall be securely deleted.
- Cryptographic keys may be destroyed where applicable.
- Media sanitization procedures shall follow approved standards.
- Destruction activities shall be documented and verified.

Destruction Standards

Destruction activities shall align with:

- NIST SP 800-88 Rev.1
- HITRUST CSF
- ISO/IEC 27001
- Organizational secure disposal requirements

Destruction Documentation

Documentation shall include:

- Backup identifier
- Archive identifier
- Date of destruction
- Destruction methodology
- Responsible personnel
- Verification results
- Supporting evidence

Validation Requirements

All destruction activities shall be:

- Documented
- Verified
- Auditable
- Approved by authorized personnel

Retention of Destruction Records

Backup destruction records shall be retained for a minimum Six (6) Years or longer where required by law, regulation, contract, audit requirements, or organizational policy.

11. Customer Offboarding, Contract Termination, and Data Disposition

11.1 Customer Offboarding and Contract Termination Policy

Policy: Cognera Health shall maintain documented, controlled, and auditable customer offboarding procedures to ensure the secure, compliant, and orderly disposition, return, transfer, retention, archival, deletion, destruction, and preservation of customer information following termination, expiration, non-renewal, suspension, migration, or other cessation of services.

Customer offboarding activities shall be performed in a manner that protects privacy, security, continuity of care, regulatory compliance, contractual obligations, legal preservation requirements, and organizational governance standards.

Offboarding procedures shall support the secure transition of customer information while ensuring that information is retained, returned, archived, deleted, anonymized, or destroyed in accordance with applicable legal, regulatory, healthcare, privacy, security, contractual, and operational requirements.

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH Act
- 45 CFR §164.308(a)(3)
- 45 CFR §164.308(a)(4)
- 45 CFR §164.310(d)
- 45 CFR §164.316
- GDPR
- UK GDPR
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- NIST Cybersecurity Framework

- NIST SP 800-88 Rev.1
- Applicable contractual obligations
- Business Associate Agreement (BAA) requirements

11.2 Customer Offboarding Governance

Policy: Upon termination or expiration of customer agreements, Cognera Health shall initiate formal customer offboarding procedures to ensure the proper handling, transfer, preservation, retention, deletion, anonymization, or destruction of customer information and related records.

Offboarding activities shall be coordinated among:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Information Security
- Customer Success
- Operations
- Data Governance Committee
- Authorized Customer Representatives

Offboarding Objectives

Customer offboarding activities shall:

- Protect customer information.
- Protect PHI and ePHI.
- Maintain continuity of care.
- Support customer transition activities.
- Fulfill contractual obligations.
- Support regulatory compliance.
- Preserve required records.
- Eliminate unauthorized access.
- Ensure secure information disposition.
- Maintain auditability and accountability.

11.3 Customer Data Export and Retrieval

Policy: Customers shall be provided a reasonable opportunity to obtain copies of their information prior to deletion, destruction, anonymization, or final disposition activities.

Data Export Services

Subject to contractual obligations and applicable laws, customers may request:

- Clinical Record Exports
- Assessment Data Exports
- Treatment Plan Exports
- Care Plan Exports
- Messaging and Communication Exports
- Audit Log Exports
- Reporting Data Exports
- Analytics Data Exports
- Operational Data Exports
- User Account Data Exports
- Consent and Authorization Records
- AI Governance Records (where applicable)
- Other customer-owned records

Export Timeframe

Customers may request exports within Sixty (60) calendar days following termination, expiration, or notice of contract cessation unless otherwise specified by contract.

Export Formats

Where technically feasible, exports may be provided in:

- Structured electronic formats
- Industry-standard formats
- Machine-readable formats
- Customer-approved formats
- Contractually specified formats

11.4 Data Retention and Disposition Following Termination

Policy: Following completion of customer offboarding activities and expiration of applicable retrieval periods, customer information shall be managed in accordance with approved retention schedules, contractual requirements, legal obligations, and regulatory requirements.

Data Disposition Activities

Customer information may be:

- Returned to the customer
- Archived
- Retained
- Deleted
- De-identified

- Anonymized
- Securely destroyed

based upon:

- Contractual requirements
- Customer instructions
- Regulatory obligations
- Healthcare record retention requirements
- Legal preservation requirements
- Organizational policies

Production Data Disposition

Unless otherwise required:

Production customer data shall be dispositioned within Ninety (90) Calendar Days following completion of customer offboarding activities.

Disposition activities may include:

- Secure deletion
- Data return
- Data migration support
- De-identification
- Anonymization
- Secure destruction

11.5 Access Revocation and Account Termination

Policy: Access to customer information, systems, applications, integrations, administrative interfaces, and associated services shall be revoked promptly following contract termination, customer offboarding, role changes, or authorized termination events.

Reference: 45 CFR §164.308(a)(3)

Procedures

Access revocation activities may include:

- User account deactivation
- Credential revocation
- API key revocation
- Integration termination
- Third-party access removal
- Administrative access removal

- Single Sign-On (SSO) termination
- Privileged access removal
- Vendor access termination

Access Revocation Timeframe

All access shall be revoked within Twenty-Four (24) Hours of approved termination or offboarding activities unless otherwise required by contract, law, or customer instruction.

Documentation

Access revocation activities shall be:

- Logged
- Audited
- Verified
- Retained for compliance purposes

11.6 Backup, Archive, and Recovery Data Handling

Policy: Backup copies, disaster recovery archives, immutable backups, and archived information may continue to exist temporarily following customer offboarding until expiration of approved retention schedules and backup lifecycle requirements.

Requirements

Backup data shall:

- Remain protected by applicable security controls.
- Remain encrypted.
- Remain subject to access controls.
- Be retained only as long as required.
- Be deleted or destroyed according to approved backup retention schedules.

Backup Disposition

Backup copies containing customer information shall be removed, overwritten, sanitized, or destroyed according to approved backup lifecycle management procedures and retention schedules.

11.7 Legal Holds and Preservation Requirements

Policy: Customer information subject to legal hold, litigation, investigation, regulatory inquiry, audit, security investigation, or preservation requirements shall not be deleted, destroyed, anonymized, or otherwise dispositioned until authorized release is provided.

Preservation Triggers

Examples include:

- Litigation
- Regulatory investigations
- OCR investigations
- Security investigations
- Compliance audits
- Customer disputes
- Contract disputes
- Government requests

Requirements

Legal holds shall supersede normal disposition schedules until released by authorized personnel.

11.8 Certificates of Destruction and Disposition Verification

Policy: Cognera Health shall provide evidence of completed destruction, deletion, anonymization, or disposition activities where contractually required, legally required, or requested by authorized customers.

Certificates of Destruction

Certificates of destruction may be provided upon request and may include:

- Customer Identifier
- Information Categories Affected
- Date of Destruction
- Destruction Methodology
- Systems Affected
- Verification Activities Performed
- Authorized Personnel
- Destruction Approval References

Verification Requirements

All disposition activities shall be:

- Documented
- Verified
- Auditable
- Approved
- Retained in accordance with applicable retention schedules

Retention of Disposition Records

Customer offboarding records, destruction records, disposition records, and related documentation shall be retained for a Minimum Six (6) Years unless a longer retention period is required by law, regulation, contract, litigation hold, or organizational policy.

11.9 Offboarding Compliance Monitoring

Policy: Cognera Health shall periodically review customer offboarding activities to ensure compliance with contractual obligations, regulatory requirements, privacy obligations, security requirements, and organizational governance standards.

Monitoring Activities

Monitoring may include:

- Offboarding reviews
- Data disposition reviews
- Access revocation reviews
- Customer transition reviews
- Compliance audits
- Security assessments
- Regulatory readiness reviews
- Corrective action reviews

Results shall be reported to appropriate governance, compliance, privacy, security, and leadership stakeholders as part of ongoing compliance monitoring and continuous improvement activities.

12. Legal Holds, Preservation Orders, and eDiscovery Requirements

12.1 Legal Hold and Preservation Policy

Policy: Cognera Health shall establish and maintain documented legal hold, records preservation, litigation readiness, and eDiscovery procedures to ensure that information subject to actual or anticipated litigation, regulatory inquiries, audits, investigations, contractual disputes, security incidents, government requests, or other preservation obligations is protected from alteration, deletion, destruction, anonymization, disposition, or unauthorized modification.

When a legal hold, preservation requirement, or eDiscovery obligation is initiated, all applicable retention schedules, deletion schedules, destruction activities, anonymization activities, and disposition procedures affecting the relevant information shall be immediately suspended until authorized release is provided.

Legal hold requirements supersede standard records retention schedules, data deletion schedules, archival disposition schedules, and customer offboarding disposition activities.

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH Act
- 45 CFR §164.308(a)(1)
- 45 CFR §164.316
- Federal Rules of Civil Procedure (FRCP)
- GDPR
- UK GDPR
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- NIST Cybersecurity Framework
- Applicable litigation, discovery, regulatory, and contractual requirements

Objectives

Legal hold and preservation activities are intended to:

- Preserve potentially relevant information.
- Prevent accidental destruction of evidence.
- Support litigation readiness.
- Support regulatory compliance.
- Support investigations and audits.
- Ensure legal defensibility.
- Reduce regulatory and legal risk.
- Maintain integrity and chain of custody of records.

12.2 Legal Hold Trigger Events

Policy: A legal hold may be initiated whenever Cognera Health becomes aware of circumstances that may require the preservation of information for legal, regulatory, contractual, investigative, audit, compliance, security, or operational purposes.

Trigger Events

Legal holds may be initiated in response to:

- Pending or anticipated litigation
- Regulatory investigations
- OCR investigations
- HHS investigations
- Government inquiries or subpoenas
- Security incidents
- Data breaches
- Privacy incidents
- Internal investigations
- Compliance investigations
- Contract disputes
- Customer disputes
- Employment disputes
- Audit findings
- Regulatory enforcement actions
- Law enforcement requests
- Preservation requests from customers or Covered Entities
- eDiscovery requests
- Legal counsel directives
- Other events requiring preservation of information

Covered Information

Legal holds may apply to:

- PHI and ePHI
- Clinical records
- Assessment records
- Communications
- Audit logs
- Security logs
- Email records
- Voice recordings
- Transcriptions
- AI governance records
- Vendor records
- Contract records
- Backup archives
- Disaster recovery archives
- Customer records

- Operational records
- Any information reasonably anticipated to be relevant to the matter under review

12.3 Legal Hold Issuance Procedures

Policy: Legal hold notices shall be issued by Legal Counsel or an authorized representative acting on behalf of Legal Counsel.

Procedures

Upon identification of a legal hold event, Legal Counsel shall:

- Evaluate preservation requirements.
- Determine the scope of information subject to preservation.
- Identify affected business units.
- Identify affected systems, applications, repositories, and storage locations.
- Identify information custodians.
- Identify third-party providers holding relevant information.
- Issue formal legal hold notices.
- Coordinate with Privacy, Compliance, Security, Operations, Engineering, and other affected stakeholders.
- Document preservation requirements.
- Establish monitoring and reporting requirements.
- Verify implementation of preservation controls.

Legal Hold Notice Requirements

Legal hold notices may include:

- Hold identifier
- Matter description
- Preservation scope
- Systems affected
- Information categories affected
- Custodians affected
- Effective date
- Preservation instructions
- Escalation procedures
- Compliance expectations

12.4 Preservation and Suspension Requirements

Policy: Upon issuance of a legal hold, all applicable deletion, destruction, anonymization, archival disposition, customer offboarding disposition, and data lifecycle management activities affecting preserved information shall be suspended.

Preservation Actions

Affected personnel shall:

- Preserve relevant information.
- Suspend deletion activities.
- Suspend destruction activities.
- Suspend anonymization activities.
- Suspend disposition activities.
- Preserve backup copies where required.
- Preserve audit records.
- Preserve security records.
- Preserve communications.
- Preserve metadata where applicable.

System Preservation Requirements

Affected systems may require:

- Retention overrides
- Backup preservation
- Archive preservation
- Snapshot preservation
- Immutable storage controls
- Enhanced monitoring
- Access restrictions
- Chain-of-custody controls

12.5 Custodian Responsibilities

Policy: Individuals identified as custodians of relevant information shall cooperate with preservation activities and comply with legal hold requirements.

Custodian Responsibilities

Custodians shall:

- Preserve identified information.
- Follow legal hold instructions.

- Refrain from deleting relevant information.
- Report potential issues affecting preservation.
- Cooperate with investigations and discovery activities.
- Participate in periodic legal hold confirmations where required.

Failure to comply with legal hold requirements may result in disciplinary action, regulatory consequences, legal sanctions, or contractual liability.

12.6 eDiscovery Management

Policy: Cognera Health shall maintain procedures supporting the identification, collection, preservation, review, export, and production of electronically stored information (ESI) when required for litigation, investigations, regulatory reviews, audits, or authorized discovery activities.

eDiscovery Activities

- eDiscovery activities may include:
- Identification of relevant information
- Custodian interviews
- Data collection
- Preservation activities
- Data processing
- Review and analysis
- Legal review
- Export and production
- Chain-of-custody documentation
- Production tracking

Sources of Electronically Stored Information (ESI)

ESI may include:

- Email
- Messaging systems
- Clinical records
- Assessments
- Voice recordings
- Audit logs
- Security logs
- AI records
- Cloud storage
- Backup systems
- Collaboration systems

- Customer records
- Operational systems

12.7 Legal Hold Monitoring and Compliance

Policy: Cognera Health shall periodically monitor legal hold compliance to ensure preservation requirements remain effective throughout the duration of the hold.

Monitoring Activities

Monitoring may include:

- Custodian confirmations
- System preservation reviews
- Retention override reviews
- Audit log reviews
- Backup preservation reviews
- Compliance assessments
- Internal audits
- Legal hold status reviews

Documentation

Legal hold records shall include:

- Hold notices
- Custodian acknowledgements
- Preservation actions
- Monitoring activities
- Compliance reviews
- Release authorizations
- Related correspondence

12.8 Legal Hold Release

Policy: Legal holds shall remain in effect until formally released by Legal Counsel.

Release Authority

Only Legal Counsel or an authorized representative designated by Legal Counsel may authorize:

- Legal hold release
- Resumption of deletion schedules
- Resumption of destruction activities
- Resumption of anonymization activities
- Final disposition of preserved information

Release Procedures

Upon release:

- Custodians shall be notified.
- Preservation overrides shall be removed.
- Retention schedules may resume.
- Disposition schedules may resume.
- Release documentation shall be retained.

12.9 Retention of Legal Hold Records

Policy: Records supporting legal hold and eDiscovery activities shall be retained to demonstrate compliance with preservation obligations and legal requirements.

Retention Period

Legal hold and eDiscovery records shall be retained for a Minimum Six (6) Years following legal hold release or final matter closure, whichever is later unless a longer retention period is required by law, regulation, court order, settlement agreement, contract, or organizational policy.

Covered Records

- Legal Hold Notices
- Preservation Orders
- Custodian Lists
- Custodian Acknowledgements
- eDiscovery Records
- Collection Records
- Production Records
- Chain-of-Custody Records
- Monitoring Records
- Release Authorizations
- Legal Hold Audit Records
- Related Legal Correspondence

13. Secure Disposal, Media Sanitization, and Information Destruction Standards

13.1 Secure Disposal and Information Destruction Policy

Policy: Cognera Health shall establish, implement, and maintain documented procedures governing the secure disposal, destruction, sanitization, decommissioning, and final disposition of

information assets, storage media, systems, backups, archives, and records containing Protected Health Information (PHI), electronic Protected Health Information (ePHI), personal information, confidential business information, security records, operational data, and other sensitive information.

Information shall be destroyed, sanitized, anonymized, de-identified, or otherwise disposed of in a manner that prevents unauthorized access, reconstruction, recovery, disclosure, reuse, modification, or retrieval.

Secure disposal activities shall be performed in accordance with approved retention schedules, legal requirements, contractual obligations, privacy requirements, security standards, records management practices, and organizational governance controls.

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH Act
- 45 CFR §164.310(d)(2)
- 45 CFR §164.312
- GDPR Article 5 (Storage Limitation)
- GDPR Article 17 (Right to Erasure)
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- NIST SP 800-88 Rev.1 Media Sanitization Guidelines
- NIST SP 800-53
- Applicable contractual obligations
- Applicable regulatory requirements

Disposal Objectives

Secure disposal activities are intended to:

- Protect confidentiality of information.
- Prevent unauthorized disclosure.
- Eliminate unnecessary retention of information.
- Reduce privacy and security risks.
- Support regulatory compliance.
- Support contractual obligations.

- Support defensible records management practices.
- Protect customer, individual, and organizational information.
- Maintain audit readiness and compliance readiness.

13.2 Information Disposition Authorization Requirements

Policy: Information shall not be destroyed, deleted, sanitized, anonymized, de-identified, or otherwise dispositioned unless authorized through approved records retention schedules, legal review processes, customer requirements, regulatory requirements, or approved disposition activities.

Pre-Disposal Validation Requirements

Prior to destruction or disposition, Cognera Health shall verify:

- Retention requirements have been satisfied.
- Legal hold requirements do not apply.
- Litigation preservation requirements do not exist.
- Regulatory preservation requirements do not exist.
- Customer contractual obligations have been satisfied.
- Business continuity requirements have been reviewed.
- Audit requirements have been reviewed.
- Data owner approval has been obtained where required.
- Disposal activities have been documented.

13.3 Electronic Data Destruction and Media Sanitization

Policy: Electronic information shall be securely deleted, destroyed, sanitized, or rendered unrecoverable using approved destruction methodologies appropriate to the sensitivity, classification, storage medium, and regulatory requirements applicable to the information.

Approved Electronic Destruction Methods

Depending on media type, risk level, and applicable requirements, approved methods may include:

Cryptographic Erasure

Destruction of encryption keys rendering protected information permanently inaccessible and unrecoverable.

Examples:

- Encrypted databases
- Cloud storage repositories
- Backup systems
- Encrypted storage volumes

Secure Overwrite

Overwriting data using approved sanitization methods that prevent recovery through commercially available recovery techniques.

Examples:

- Hard drives
- Storage arrays
- Temporary storage systems

Secure Cloud Destruction

Deletion and sanitization of cloud-hosted information through approved cloud provider destruction procedures.

Examples:

- Cloud databases
- Object storage
- Backup repositories
- Disaster recovery environments

Media Sanitization

Sanitization techniques consistent with NIST SP 800-88 Rev.1 guidance.

Examples:

- Logical sanitization
- Purging
- Cryptographic sanitization
- Platform-specific sanitization controls

Encryption Key Destruction

Permanent destruction of encryption keys used to protect information, rendering associated information permanently inaccessible.

Covered Electronic Information

Examples include:

- PHI and ePHI
- Clinical records
- Assessment records
- Audit logs

- Security logs
- Backup archives
- AI governance records
- Analytics data
- Operational records
- Customer records
- Employee records
- Vendor records
- Email records
- Messaging records

13.4 Physical Media, Electronic Storage Media, and Hardware Destruction Standards

Policy: Cognera Health shall securely sanitize, destroy, decommission, dispose of, or otherwise render unrecoverable any physical media, electronic storage media, hardware, devices, systems, appliances, and technology assets containing Protected Health Information (PHI), electronic Protected Health Information (ePHI), personal information, confidential business information, security records, customer information, audit records, backup data, or other regulated information.

Destruction and disposal activities shall be performed using approved methodologies designed to prevent unauthorized access, disclosure, reconstruction, recovery, retrieval, reuse, modification, or distribution of information.

Approved Physical and Electronic Destruction Methods

Depending on media type, sensitivity, classification level, and regulatory requirements, approved destruction methods may include:

- **Shredding**
  - Secure destruction of paper records, printed materials, removable media, optical media, and other physical records using approved shredding processes.
- **Pulverization**
  - Mechanical destruction reducing media into particles or fragments that prevent reconstruction or recovery.
- **Crushing and Physical Destruction**
  - Physical destruction of hard drives, solid-state drives, storage devices, and other media using approved destruction equipment.
- **Incineration**
  - Destruction through approved incineration processes where legally permissible and environmentally appropriate.

- **Cryptographic Erasure**
  - Permanent destruction of encryption keys rendering encrypted information inaccessible and unrecoverable.
- **Media Sanitization**
  - Sanitization methods consistent with NIST SP 800-88 Rev.1 guidance, including clearing, purging, and cryptographic sanitization.
- **Certified Third-Party Destruction Services**
  - Use of approved destruction providers capable of maintaining chain-of-custody controls and providing destruction certifications.
- **Covered Physical Media**

  Examples include:
  - Paper Records
  - Printed Reports
  - Signed Authorizations
  - Consent Forms
  - Contracts and Agreements
  - Training Records
  - Compliance Documentation
  - Audit Documentation
  - Printed PHI and Clinical Records
- **Covered Electronic Storage Media and Devices**

  Examples include:
  - Hard Disk Drives (HDD)
  - Solid State Drives (SSD)
  - USB Flash Drives
  - Portable Storage Devices
  - Removable Media
  - Backup Tapes
  - Optical Media
  - Memory Cards
  - Mobile Devices
  - Smartphones
  - Tablets
  - Laptops
  - Workstations
  - Servers
  - Storage Appliances
  - Network Attached Storage (NAS)
  - Storage Area Networks (SAN)
  - Backup Appliances
  - Security Appliances
  - Virtualization Hosts
  - Decommissioned Hardware

  - Customer-Dedicated Equipment
- **Covered Cloud and Virtual Storage Environments**

  Examples include:
  - Cloud Databases
  - Cloud Storage Services
  - Object Storage Repositories
  - Data Lakes
  - Data Warehouses
  - Backup Repositories
  - Snapshot Repositories
  - Archive Storage
  - Disaster Recovery Environments
  - Virtual Machines
  - Container Storage
  - Kubernetes Persistent Volumes
  - SaaS Data Repositories
  - AI Data Repositories
  - Analytics Platforms
  - Customer Data Stores
- Chain-of-Custody Requirements

  All destruction activities shall maintain documented chain-of-custody controls including:
  - Asset Identification
  - Information Classification
  - Custodian Identification
  - Transfer Records
  - Destruction Authorization
  - Destruction Methodology
  - Verification Records
  - Certificate of Destruction (where applicable)
- **Verification Requirements**

  All destruction, sanitization, disposal, and decommissioning activities shall be:
  - Authorized
  - Logged
  - Documented
  - Verified
  - Audited
  - Approved

Retention of Destruction Records

Records supporting destruction and disposal activities shall be retained is Minimum Six (6) Years unless a longer retention period is required by law, regulation, contract, litigation hold, or organizational policy.

13.5 De-Identification and Anonymization

Policy: Where deletion or destruction is not required, Cognera Health may utilize approved de-identification or anonymization techniques to remove identifying elements from information.

Approved Methods

- **HIPAA Safe Harbor:** Removal of identifiers in accordance with 45 CFR §164.514.
- **Expert Determination:** De-identification validated by a qualified expert.
- **Anonymization:** Irreversible removal of identifiers such that individuals can no longer be identified.
- **Requirements:** De-identification and anonymization activities shall be:
  - Documented
  - Validated
  - Auditable
  - Approved
  - Periodically reviewed

13.6 Disposal Verification and Validation

Policy: All destruction, deletion, sanitization, anonymization, and disposition activities shall undergo validation and verification to confirm successful completion.

Verification Activities

Verification may include:

- Automated validation
- Destruction reporting
- System validation testing
- Media sanitization review
- Audit log review
- Compliance review
- Sampling and testing
- Third-party attestation review

Destruction Documentation

Documentation may include:

- Destruction request identifier
- Information category
- Media type
- Disposal method

- Date of destruction
- Responsible personnel
- Validation results
- Supporting evidence
- Approval records

13.7 Certificates of Destruction

Policy: Where required by law, regulation, contract, customer request, audit requirement, or organizational policy, Cognera Health shall maintain and/or provide certificates of destruction.

Certificate Information

Certificates may include:

- Destruction reference number
- Date of destruction
- Information category
- Media type
- Destruction methodology
- Responsible personnel
- Validation results
- Authorized approvals
- Third-party attestations where applicable

13.8 Disposal Monitoring, Auditing, and Compliance Oversight

Policy: Secure disposal activities shall be periodically reviewed to ensure compliance with privacy, security, retention, destruction, records management, and regulatory requirements.

Monitoring Activities

Monitoring may include:

- Disposal audits
- Media sanitization reviews
- Vendor destruction reviews
- Retention schedule compliance reviews
- Destruction verification reviews
- Chain-of-custody reviews
- Regulatory compliance reviews
- Security assessments

Governance Oversight

Oversight may involve:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Information Security
- Data Governance Committee
- Internal Audit

13.9 Approval Requirements

Policy: All destruction, deletion, sanitization, and disposition activities shall be:

- Authorized
- Documented
- Logged
- Verified
- Audited
- Approved

by appropriate personnel based on the sensitivity, classification, and regulatory requirements applicable to the information being dispositioned.

Retention of Disposal Records

Records supporting secure disposal activities shall be retained for is Minimum Six (6) Years unless a longer retention period is required by law, regulation, contract, legal hold, audit requirement, or organizational policy.

14. Vendor, Business Associate, and Subcontractor Data Disposition Requirements

14.1 Vendor and Third-Party Data Disposition Policy

Policy: Cognera Health shall require Business Associates (BAs), subcontractors, vendors, Cloud Service Providers (CSPs), Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), consultants, contractors, and other third-party service providers that create, receive, maintain, process, store, transmit, archive, or dispose of information on behalf of Cognera Health to comply with applicable information retention, preservation, deletion, destruction, secure disposal, privacy, security, and regulatory requirements.

Third-party organizations shall maintain controls designed to protect Protected Health Information (PHI), electronic Protected Health Information (ePHI), personal information, confidential business

information, security records, customer information, backup data, audit records, and other regulated information throughout the information lifecycle.

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH Act
- 45 CFR §164.308(b) Business Associate Requirements
- 45 CFR §164.502(e)
- 45 CFR §164.504(e)
- GDPR
- UK GDPR
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- NIST Cybersecurity Framework
- NIST SP 800-88 Rev.1
- Applicable contractual and regulatory requirements

Objectives

Vendor data disposition controls are intended to:

- Protect regulated information.
- Reduce privacy and security risks.
- Ensure proper retention and destruction practices.
- Support regulatory compliance.
- Ensure accountability across third-party relationships.
- Maintain audit readiness.
- Support customer and contractual obligations.
- Ensure secure disposition of information at the conclusion of services.

14.2 Contractual and Business Associate Agreement Requirements

Policy: Contracts, Business Associate Agreements (BAAs), Data Processing Agreements (DPAs), Master Service Agreements (MSAs), Statements of Work (SOWs), and other vendor agreements shall include provisions governing information retention, preservation, return, destruction, disposal, privacy, security, and audit rights.

Required Contractual Provisions

Where applicable, agreements shall address:

- Data ownership requirements
- Information retention requirements
- Data return requirements
- Data export requirements
- Secure destruction requirements
- Media sanitization requirements
- Privacy requirements
- Security requirements
- Breach notification obligations
- Regulatory compliance requirements
- Audit and assessment rights
- Legal hold requirements
- Subcontractor obligations
- Data disposition procedures
- Certificate of destruction requirements
- Termination assistance requirements
- Customer-directed disposition requirements

Business Associate Requirements

Business Associates and subcontractors handling PHI or ePHI shall:

- Execute appropriate BAAs.
- Implement HIPAA-compliant safeguards.
- Support customer information disposition requirements.
- Cooperate with compliance reviews and audits.
- Notify Cognera Health of material security or privacy incidents.
- Maintain documented retention and destruction procedures.

14.3 Vendor Data Return and Preservation Requirements

Policy: Upon contract expiration, termination, migration, replacement, or cessation of services, vendors shall return, preserve, archive, delete, destroy, de-identify, anonymize, or otherwise disposition information in accordance with contractual obligations and applicable legal requirements.

Data Return Requirements

Where applicable, vendors shall support:

- Data exports
- Clinical record exports

- Assessment exports
- Audit log exports
- Security log exports
- Backup exports
- Reporting exports
- Analytics exports
- Operational data exports
- Customer-directed transfers

Preservation Requirements

Vendors shall preserve information where required by:

- Legal holds
- Litigation
- Regulatory investigations
- Security investigations
- Contractual obligations
- Customer requirements
- Applicable laws and regulations

14.4 Vendor Secure Disposal Requirements

Policy: Vendors shall securely dispose of information, media, systems, backups, archives, and storage repositories containing regulated or confidential information in accordance with approved destruction standards and contractual requirements.

Approved Vendor Disposal Activities

Examples include:

- Secure deletion
- Cryptographic erasure
- Media sanitization
- Secure destruction
- Backup expiration processing
- Archive destruction
- De-identification
- Anonymization
- Physical media destruction

Destruction Standards

Vendor disposal activities should align with:

- NIST SP 800-88 Rev.1
- HIPAA Security Rule requirements
- HITRUST CSF
- ISO/IEC 27001
- Industry-recognized disposal practices

Documentation Requirements

Vendors shall maintain evidence supporting:

- Destruction activities
- Sanitization activities
- Deletion activities
- Media disposal activities
- Backup disposition activities
- Verification activities

14.5 Vendor Termination and Offboarding Procedures

Policy: Upon termination, expiration, non-renewal, or replacement of a vendor relationship, Cognera Health shall execute documented vendor offboarding procedures to ensure information remains protected and disposition activities are completed appropriately.

Termination Activities

Within thirty (30) calendar days, unless otherwise specified by contract or legal requirement, Cognera Health shall:

- Revoke system access.
- Disable accounts and credentials.
- Revoke API access.
- Remove administrative privileges.
- Terminate integrations and connections.
- Review vendor-held information.
- Verify information return activities.
- Verify preservation requirements.
- Verify secure destruction activities.
- Obtain destruction certifications where applicable.
- Update vendor inventories.
- Update asset inventories.
- Update risk management records.
- Document offboarding completion.

Access Revocation Requirements

Vendor access shall be revoked in accordance with:

- 45 CFR §164.308(a)(3)
- Organizational access management requirements
- Vendor offboarding procedures

14.6 Vendor Attestations and Certificates of Destruction

Policy: Cognera Health may require vendors to provide written attestations, certifications, reports, or evidence demonstrating completion of information disposition activities.

Acceptable Evidence

Examples include:

- Certificate of Destruction
- Media Sanitization Report
- Disposal Verification Report
- Secure Deletion Attestation
- Audit Report
- Compliance Certification
- Third-Party Assessment Report
- Data Return Confirmation
- Data Destruction Confirmation

Required Information

Documentation may include:

- Vendor Name
- Information Categories Affected
- Systems Affected
- Destruction Methodology
- Date of Destruction
- Authorized Personnel
- Validation Activities
- Compliance References

14.7 Vendor Monitoring and Compliance Oversight

Policy: Cognera Health shall periodically assess vendor compliance with retention, deletion, destruction, privacy, security, and information governance requirements.

Monitoring Activities

Monitoring may include:

- Vendor Risk Assessments
- Compliance Reviews
- Security Reviews
- Audit Activities
- BAA Reviews
- Contract Reviews
- Destruction Verification Reviews
- Regulatory Compliance Reviews
- Third-Party Assessments

Documentation Retention

Vendor disposition records, destruction attestations, audit records, compliance reviews, and related documentation shall be retained for is Minimum Six (6) Years unless a longer retention period is required by law, regulation, contract, legal hold, customer requirement, or organizational policy.

15. Monitoring, Auditing, Compliance Validation, and Continuous Oversight

15.1 Monitoring, Auditing, and Compliance Validation Policy

Policy: Cognera Health shall maintain a comprehensive monitoring, auditing, compliance validation, and governance oversight program designed to evaluate the effectiveness of information retention, deletion, destruction, legal hold, records management, privacy, security, data governance, and regulatory compliance controls.

Monitoring and auditing activities shall provide reasonable assurance that information lifecycle management processes operate effectively, regulatory requirements are satisfied, retention schedules are enforced, deletion and destruction activities are properly executed, and organizational policies are consistently followed.

Monitoring and compliance validation activities shall support continuous improvement, risk management, audit readiness, regulatory readiness, and operational accountability.

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH Act

- 45 CFR §164.308(a)(1)(ii)(D)
- 45 CFR §164.308(a)(8)
- GDPR Accountability Principles
- GDPR Article 5
- GDPR Article 24
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001
- ISO/IEC 27701
- NIST Cybersecurity Framework
- NIST SP 800-53
- Applicable contractual and regulatory requirements

15.2 Monitoring Activities

Policy: Cognera Health shall perform ongoing monitoring activities designed to identify compliance gaps, operational deficiencies, unauthorized activities, retention schedule violations, security concerns, and records management issues.

Monitoring Activities

Monitoring activities may include:

Daily Monitoring

- Security log reviews
- Audit log reviews
- Deletion activity reviews
- Access monitoring
- Security event monitoring
- Retention exception monitoring
- Legal hold monitoring
- Backup monitoring
- Vendor activity monitoring

Weekly Monitoring

- Compliance reviews
- Access control reviews
- Deletion request status reviews
- Open legal hold reviews
- Incident tracking reviews
- Vendor compliance reviews

Monthly Monitoring

- Records retention reviews
- Data lifecycle management reviews
- Data disposition reviews
- Destruction activity reviews
- Backup retention reviews
- Compliance metrics reviews
- Risk monitoring reviews
- Governance reporting reviews

Quarterly Monitoring

- Internal compliance audits
- Retention schedule audits
- Legal hold audits
- Vendor compliance audits
- Privacy reviews
- Security reviews
- Data governance reviews
- Records management assessments

Annual Monitoring

- Independent compliance assessments
- Internal control evaluations
- Regulatory readiness reviews
- Governance program reviews
- Risk assessments
- Audit program reviews
- Policy effectiveness reviews
- Continuous improvement assessments

15.3 Compliance Validation Activities

Policy: Cognera Health shall periodically validate that information lifecycle management controls are operating effectively and in accordance with regulatory, contractual, legal, privacy, security, and organizational requirements.

Validation Activities

Validation activities may include:

- Retention schedule compliance testing

- Deletion verification testing
- Secure destruction validation
- Legal hold effectiveness reviews
- Backup retention validation
- Vendor compliance validation
- Access control validation
- Audit trail validation
- Chain-of-custody validation
- Policy adherence reviews
- Regulatory compliance assessments

Review Scope

Reviews may evaluate:

- Information inventories
- Retention schedules
- Deletion activities
- Destruction activities
- Archival processes
- Preservation activities
- Legal hold management
- Vendor disposition activities
- Security controls
- Privacy controls

15.4 Audit Program

Policy: Cognera Health shall maintain an audit program designed to assess compliance with approved retention schedules, destruction requirements, legal hold procedures, regulatory requirements, contractual obligations, and organizational policies.

Audit Types

Examples include:

- Internal Audits
- Compliance Audits
- Privacy Audits
- Security Audits
- Records Management Audits
- Vendor Audits
- Third-Party Assessments

- Regulatory Readiness Reviews
- Risk-Based Audits

Audit Activities

Audits may review:

- Retention compliance
- Deletion compliance
- Destruction validation
- Legal hold compliance
- Backup management
- Vendor disposition activities
- Audit trail integrity
- Governance effectiveness
- Corrective action implementation

15.5 Corrective Action and Remediation

Policy: Deficiencies identified through monitoring, audits, compliance reviews, investigations, or assessments shall be documented, prioritized, tracked, and remediated in a timely manner.

Remediation Activities

May include:

- Root cause analysis
- Corrective action plans
- Control improvements
- Process improvements
- Policy updates
- Training enhancements
- Vendor remediation activities
- Security control improvements
- Governance enhancements

Tracking Requirements

Corrective actions shall include:

- Issue description
- Risk rating
- Owner assignment
- Target completion date
- Validation activities

- Closure documentation

15.6 Evidence Retention and Audit Documentation

Policy: Cognera Health shall maintain documentation sufficient to demonstrate compliance with information retention, deletion, destruction, legal hold, records management, privacy, security, and governance requirements.

Compliance Evidence

Examples include:

- Deletion Logs
- Deletion Verification Reports
- Destruction Certificates
- Media Sanitization Records
- Retention Schedule Reviews
- Retention Compliance Reports
- Legal Hold Notices
- Legal Hold Release Documentation
- Preservation Records
- Audit Reports
- Compliance Reviews
- Monitoring Reports
- Corrective Action Records
- Vendor Attestations
- Data Destruction Certifications
- Chain-of-Custody Records
- Backup Retention Reviews
- Governance Committee Records
- Regulatory Correspondence

Retention Period

Compliance evidence, monitoring records, audit records, legal hold records, destruction records, and related documentation shall be retained for is Minimum Six (6) Years unless a longer retention period is required by law, regulation, contract, litigation hold, regulatory inquiry, audit requirement, or organizational policy.

15.7 Reporting and Governance Oversight

Policy: Results of monitoring, auditing, compliance validation, and assessment activities shall be reported to appropriate governance, compliance, privacy, security, operational, and executive stakeholders.

Reporting Activities

Reports may include:

- Compliance metrics
- Audit findings
- Retention exceptions
- Legal hold status
- Deletion activity summaries
- Destruction activity summaries
- Vendor compliance status
- Risk management updates
- Corrective action status
- Regulatory readiness assessments

Governance Oversight

Oversight may be provided by:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Information Security
- Data Governance Committee
- Executive Leadership
- Internal Audit

The results of monitoring, auditing, and compliance validation activities shall be incorporated into ongoing risk management, governance reviews, policy updates, and continuous improvement initiatives.

16. Compliance Metrics, Key Performance Indicators (KPIs), and Program Effectiveness Monitoring

16.1 Compliance Performance Measurement Policy

Policy: Cognera Health shall establish, maintain, monitor, and periodically review Key Performance Indicators (KPIs), compliance metrics, operational measurements, risk indicators, and governance effectiveness measures to evaluate the performance, effectiveness, maturity, and ongoing compliance of its Data Retention, Deletion, Secure Disposal, Records Management, Privacy, Security, Information Governance, and Regulatory Compliance Programs.

Compliance metrics shall be used to:

- Measure policy effectiveness.
- Validate regulatory compliance.
- Monitor operational performance.
- Identify compliance risks and gaps.
- Support continuous improvement initiatives.
- Support governance oversight.
- Demonstrate audit readiness.
- Measure vendor and third-party compliance.
- Support executive reporting and decision-making.
- Monitor adherence to contractual, legal, regulatory, and organizational requirements.

Governance Oversight

Compliance metrics shall be reviewed by appropriate stakeholders including:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Information Security
- Data Governance Committee
- Executive Leadership

Results shall be incorporated into compliance reviews, risk assessments, audit activities, governance meetings, corrective action plans, and continuous improvement initiatives.

16.2 Compliance and Operational KPIs

KPI	Target	Frequency	Owner

Privacy Rights Requests Completed Within SLA	≥95%	Monthly	Privacy Officer
Privacy Rights Request Response Time	≤30 Days	Monthly	Privacy Officer
Deletion Requests Completed Within SLA	≥95%	Monthly	Privacy Officer
Deletion Request Completion Time	≤30 Days	Monthly	Privacy Officer
Data Retention Schedule Compliance	≥99%	Quarterly	Data Governance Committee
Retention Exception Review Completion	100%	Quarterly	Compliance Officer
Secure Disposal Verification Rate	100%	Quarterly	Compliance Officer
Destruction Documentation Completion	100%	Quarterly	Compliance Officer
Backup Retention Compliance	100%	Monthly	Information Security
Backup Destruction Compliance	100%	Quarterly	Information Security
Disaster Recovery Archive Compliance	100%	Quarterly	Information Security
Legal Hold Compliance Rate	100%	Monthly	Legal Counsel
Legal Hold Acknowledgement Completion	100%	Monthly	Legal Counsel
Legal Hold Review Completion	100%	Quarterly	Legal Counsel
Vendor Destruction Attestation Completion	100%	Quarterly	Vendor Management
Vendor Offboarding Compliance	100%	Quarterly	Vendor Management
Vendor Data Return Verification	100%	Quarterly	Vendor Management
Vendor Risk Review Completion	100%	Annually	Vendor Management
Customer Offboarding Completion	≤90 Days	Monthly	Operations
Customer Data Export Completion	≤30 Days	Monthly	Operations
Access Revocation Following Termination	≤24 Hours	Monthly	Information Security
Retention Audit Completion	Quarterly	Quarterly	Compliance Officer
Internal Compliance Review Completion	Quarterly	Quarterly	Compliance Officer
Independent Compliance Assessment Completion	Annually	Annually	Compliance Officer
Policy Review Completion	Annually	Annually	Data Governance Committee

Records Destruction Validation Completion	100%	Quarterly	Compliance Officer
Data Inventory Review Completion	100%	Quarterly	Data Governance Committee
Regulatory Inquiry Response Timeliness	≤ Required Regulatory Timeline	As Needed	Compliance Officer
Corrective Action Closure Rate	100% of Critical Findings Within 30 Days	Monthly	Compliance Officer
Audit Finding Remediation Completion	100%	Quarterly	Compliance Officer
Compliance Evidence Availability	100%	Quarterly	Compliance Officer

16.3 Information Governance Metrics

The following metrics may be utilized to evaluate overall information governance effectiveness:

- Percentage of records assigned to approved retention schedules.
- Percentage of information repositories inventoried and classified.
- Percentage of deletion activities validated and documented.
- Percentage of disposition activities completed according to schedule.
- Percentage of legal holds properly implemented.
- Percentage of archived information reviewed according to schedule.
- Percentage of vendor repositories covered by retention and destruction requirements.
- Percentage of customer offboarding activities completed according to policy.
- Percentage of cloud storage repositories subject to retention controls.
- Percentage of backup repositories compliant with retention requirements.

16.4 Privacy and Regulatory Compliance Metrics

The following metrics may be utilized to evaluate privacy compliance performance:

- Privacy rights request volume.
- Privacy rights request completion rate.
- Deletion request completion rate.
- Data portability request completion rate.
- Privacy complaint volume.
- Regulatory inquiry volume.

- Regulatory response timeliness.
- GDPR compliance review completion.
- CCPA/CPRA compliance review completion.
- HIPAA compliance review completion.
- Privacy training completion rate.

16.5 Secure Disposal and Destruction Metrics

The following metrics may be utilized to evaluate secure disposal effectiveness:

- Destruction verification completion rate.
- Destruction documentation completion rate.
- Certificate of destruction completion rate.
- Media sanitization completion rate.
- Backup destruction completion rate.
- Cloud repository destruction validation rate.
- Physical media destruction validation rate.
- Vendor destruction attestation completion rate.
- Secure disposal audit completion rate.
- Secure disposal exception rate.

16.6 Continuous Improvement Metrics

Metrics shall be periodically reviewed to:

- Identify trends.
- Identify recurring issues.
- Evaluate control effectiveness.
- Support risk management.
- Improve operational efficiency.
- Improve regulatory readiness.
- Improve governance maturity.
- Improve customer trust and transparency.

Results shall be incorporated into compliance reviews, audit programs, governance meetings, policy updates, training initiatives, risk assessments, and continuous improvement programs.

17. Continuous Improvement, Governance Maturity, and Program Enhancement

17.1 Continuous Improvement Policy

Policy: Cognera Health shall maintain a continuous improvement program designed to enhance the effectiveness, maturity, scalability, and regulatory readiness of its information governance, records management, data retention, deletion, secure disposal, privacy, security, compliance, artificial intelligence governance, risk management, and operational control programs.

Continuous improvement activities shall be integrated into governance, compliance, risk management, audit, security, privacy, operational, and organizational processes to ensure that policies, procedures, controls, technologies, and governance practices remain effective, appropriate, and aligned with evolving legal, regulatory, contractual, security, privacy, and business requirements.

The objective of continuous improvement is to proactively identify opportunities to strengthen governance effectiveness, reduce risk, improve operational efficiency, enhance regulatory compliance, increase organizational maturity, and support customer trust.

Regulatory and Standards Alignment

This policy supports applicable requirements arising from:

- HIPAA Security Rule
- 45 CFR §164.308(a)(1) Security Management Process
- 45 CFR §164.308(a)(8) Evaluation
- HIPAA Privacy Rule
- HITECH Act
- GDPR Accountability Principles
- GDPR Article 24
- CCPA / CPRA
- HITRUST Common Security Framework (CSF)
- ISO/IEC 27001 Continual Improvement Requirements
- ISO/IEC 27701
- NIST Cybersecurity Framework
- NIST Risk Management Framework
- NIST AI Risk Management Framework
- Applicable contractual and regulatory obligations

17.2 Continuous Improvement Objectives

Cognera Health shall continuously evaluate and improve:

- Information governance practices
- Records management controls
- Retention schedules
- Data deletion procedures
- Secure disposal controls
- Legal hold procedures
- Privacy compliance activities
- Security controls
- AI governance practices
- Vendor oversight processes
- Customer offboarding procedures
- Audit and monitoring activities
- Compliance reporting
- Risk management processes
- Training and awareness programs
- Operational effectiveness
- Regulatory readiness
- Governance maturity

17.3 Continuous Improvement Activities

Governance Reviews

Cognera Health shall periodically review:

- Governance frameworks
- Policies
- Procedures
- Standards
- Guidelines
- Control effectiveness
- Risk management practices
- Compliance programs

Regulatory Monitoring

Cognera Health shall continuously monitor and evaluate:

- OCR guidance and enforcement actions

- HHS guidance and regulatory updates
- HIPAA developments
- HITECH developments
- GDPR developments
- UK GDPR developments
- CCPA / CPRA developments
- State privacy law developments
- Consumer health privacy law developments
- Cybersecurity regulatory developments
- Artificial intelligence regulatory developments
- Industry standards and best practices

Audit and Assessment Reviews

Continuous improvement activities shall incorporate:

- Internal audit findings
- External audit findings
- Compliance assessments
- Risk assessments
- Penetration testing results
- Security assessments
- Privacy reviews
- Vendor assessments
- Regulatory reviews
- Customer audit findings
- Independent assessments

Incident and Investigation Reviews

Lessons learned shall be incorporated from:

- Security incidents
- Privacy incidents
- Data breaches
- Compliance investigations
- Regulatory inquiries
- Vendor incidents
- Customer complaints
- Operational issues
- AI governance incidents
- Root cause analyses

17.4 Retention Schedule and Lifecycle Management Improvements

Policy: Cognera Health shall periodically evaluate retention schedules and information lifecycle management practices to ensure continued compliance and operational effectiveness.

Review Activities

Review activities may include:

- Retention schedule effectiveness reviews
- Information inventory reviews
- Data classification reviews
- Data minimization reviews
- Disposition reviews
- Archival reviews
- Legal hold reviews
- Destruction methodology reviews
- Backup lifecycle reviews

Updates

Retention schedules shall be updated following:

- Regulatory changes
- Legal changes
- Contractual changes
- Customer requirements
- Audit findings
- Organizational changes
- Technology changes
- Business process changes

17.5 Secure Disposal and Destruction Program Improvements

Policy: Cognera Health shall periodically evaluate secure disposal practices to ensure destruction methodologies remain effective and aligned with evolving technology, regulations, threats, and industry standards.

Review Activities

Review activities may include:

- Destruction methodology reviews
- Media sanitization reviews
- NIST SP 800-88 updates

- Cloud disposal reviews
- Vendor destruction reviews
- Backup destruction reviews
- Decommissioning reviews
- Disposal audit reviews

Improvement Areas

Improvements may include:

- New destruction technologies
- Enhanced validation procedures
- Improved auditability
- Enhanced documentation controls
- Vendor management enhancements
- Automation opportunities

17.6 Privacy and Data Protection Program Improvements

Policy

Cognera Health shall periodically review privacy and data protection controls to ensure ongoing compliance with applicable privacy regulations and customer expectations.

Review Areas

- Privacy rights management
- Consent management
- Authorization management
- Disclosure management
- Data minimization practices
- Data subject request processing
- Privacy impact assessments
- Data sharing controls
- Cross-border data processing controls

17.7 Artificial Intelligence Governance Improvements

Policy: Cognera Health shall continuously evaluate and improve AI governance practices to support responsible, transparent, secure, and compliant use of artificial intelligence technologies.

Review Activities

- AI governance reviews
- AI risk assessments

- Bias monitoring reviews
- Explainability reviews
- Human oversight reviews
- Model performance reviews
- AI incident reviews
- Regulatory monitoring
- Emerging AI standards reviews

17.8 Training and Awareness Improvements

Policy

Training programs shall be periodically reviewed and updated to address evolving risks, regulations, technologies, governance requirements, and organizational needs.

Review Areas

- Retention requirements
- Deletion procedures
- Secure disposal practices
- Legal hold requirements
- Privacy requirements
- Security requirements
- AI governance requirements
- Vendor management requirements
- Regulatory updates

17.9 Continuous Improvement Reporting

Policy: Results of continuous improvement activities shall be documented, tracked, reported, and reviewed through established governance processes.

Reporting Activities

Reports may include:

- Improvement initiatives
- Audit findings
- Risk trends
- Regulatory updates
- Control enhancements
- Policy updates
- Remediation status
- Compliance metrics

- Governance maturity assessments
- Program effectiveness evaluations

Governance Oversight

Continuous improvement activities shall be reviewed by:

- Privacy Officer
- Compliance Officer
- Legal Counsel
- Information Security
- Data Governance Committee
- Executive Leadership

Results shall be incorporated into governance reviews, risk management activities, policy updates, compliance programs, and strategic planning initiatives to support ongoing regulatory readiness, operational excellence, and organizational maturity.

18. Glossary

- **Workforce:** Employees, contractors, temporary personnel, volunteers, and authorized third parties with access to organizational information.
- **BA (Business Associate):** Entity that performs services involving PHI on behalf of a Covered Entity.
- **BYOD:** Personally owned devices authorized for business use.
- **ePHI:** Protected Health Information stored, transmitted, or processed electronically.
- **HIPAA:** U.S. law governing healthcare privacy and security requirements.
- **MFA:** Authentication requiring two or more verification methods.
- **PHI:** Individually identifiable health information protected under HIPAA.
- **RBAC:** Access control based on assigned roles and responsibilities.
- **TLS:** Encryption protocol used to secure data transmission.
- **TPO:** Treatment, Payment, and Healthcare Operations activities permitted under HIPAA.
- **CSP:** Cloud Service Provider.
- **MSP:** Managed Service Provider.
- **MSSP:** Managed Security Service Provider.
- **NIST:** U.S. standards organization providing cybersecurity and privacy guidance.
- **SIEM:** Platform used for monitoring, correlating, and analyzing security events.
- **HITRUST:** Security and privacy framework commonly used within healthcare.
- **HITECH:** U.S. law strengthening HIPAA privacy, security, and breach notification requirements.

- **RTO (Recovery Time Objective):** Target time to restore systems following a disruption.
- **RPO (Recovery Point Objective):** Maximum acceptable amount of data loss following a disruption.
- **OCR:** Office for Civil Rights, the HIPAA enforcement agency within HHS.
- **HHS:** U.S. Department of Health and Human Services.
- **Covered Entity:** Healthcare organization subject to HIPAA requirements.
- **Security Incident:** Actual or attempted unauthorized access, use, disclosure, modification, destruction, or disruption of information systems.
- **Safe Harbor (De-Identification):** HIPAA method for removing specified identifiers from PHI.
- **Expert Determination:** HIPAA-approved de-identification method performed by a qualified expert.
- **AI (Artificial Intelligence):** Technology that generates insights, predictions, recommendations, or automated outputs from data.
- **Voice-to-Text:** Technology that converts spoken language into written text.
- **Human-in-the-Loop:** Human review, validation, or approval of automated or AI-generated outputs.
- **Data Retention:** Maintenance of information for a defined period.
- **Secure Disposal:** Approved destruction or sanitization of information preventing recovery or reconstruction.
- **Legal Hold:** Suspension of normal deletion or destruction activities due to legal, regulatory, audit, or investigation requirements.
- **Data Subject:** Individual whose personal data is processed.
- **Data Controller:** Entity determining why and how personal data is processed.
- **Data Processor:** Entity processing personal data on behalf of another organization.
- **Anonymization:** Irreversible removal of identifying information.
- **De-Identification:** Removal of identifiers to reduce the ability to identify an individual.
- **Deletion Request:** Request to erase, remove, or dispose of information where legally permissible.
- **Certificate of Destruction:** Document confirming secure destruction or disposal of information.
- **Audit Log:** Record of system, user, or security activities.
- **Compliance Review:** Assessment of adherence to regulatory, contractual, or organizational requirements.
- **Data Governance:** Framework for managing information throughout its lifecycle.
- **Information Asset:** Any record, system, application, database, file, or repository containing organizational information.
- **Records Management:** Administration of information from creation through final disposition.
- **Backup:** Copy of information maintained for recovery or preservation purposes.

- **Archive:** Information retained for historical, legal, regulatory, or operational purposes.
- **eDiscovery:** Identification, preservation, collection, review, and production of electronically stored information for legal or regulatory purposes.
- **Privacy Rights Request:** Request to access, correct, delete, restrict, or obtain personal information.
- **Chain of Custody:** Documentation showing control, transfer, and handling of information or media.
- **Media Sanitization:** Process of removing information from storage media to prevent recovery.
- **Business Continuity:** Capability to maintain critical operations during and after a disruption.
- **Disaster Recovery:** Processes used to restore systems, services, and information following a disruption.

Appendix A – Data Retention Summary Matrix

Section	Category	Retention Requirement
4.2	Clinical Records	7 years after last clinical activity, encounter, service, or documented interaction unless longer retention is required by law, contract, payer, accreditation, litigation hold, regulatory investigation, or customer requirements
4.3	Assessments and Measurement Instruments	7 years or longer if required by law, regulation, contract, accreditation, payer, or customer requirements
4.4	Messaging and Communication Records	7 years or longer if required by applicable retention requirements
4.5	Authorizations and Consents	6 years from creation date or last effective date, whichever is later
4.6	Disclosure Records	6 years
4.7	Audit Logs	6 years
4.7	Authentication Logs	6 years
4.7	Access Logs	6 years
4.7	Security Event Logs	6 years
4.7	SIEM Records	6 years
4.7	Security Incident Records	6 years
4.7	Breach Investigation Records	6 years
4.7	Vulnerability Assessments	6 years
4.7	Vulnerability Scans	6 years

4.7	Penetration Test Reports	6 years
4.7	Risk Assessments	6 years
4.7	Security Monitoring Reports	6 years
4.7	Threat Intelligence Records	6 years
4.7	Compliance Monitoring Records	6 years
4.8	Policies	6 years
4.8	Procedures	6 years
4.8	HIPAA Training Records	6 years
4.8	Compliance Training Records	6 years
4.8	Business Associate Agreements (BAAs)	6 years after termination
4.8	Compliance Reviews	6 years
4.8	Internal Audit Reports	6 years
4.8	External Audit Reports	6 years
4.8	OCR Correspondence	6 years
4.8	Regulatory Inquiry Records	6 years
4.8	Corrective Action Plans	6 years
4.8	Governance Committee Records	6 years
4.8	Risk Management Reviews	6 years
4.8	AI Governance Records	6 years
5.1	Privacy Rights Requests	Retained according to approved retention schedules; recommended minimum 6 years
6.3	Deletion Evidence and Deletion Logs	6 years minimum
6.4	Deletion Requests	6 years minimum
6.5	Deletion Denials and Exception Documentation	6 years minimum
7.2	HIPAA Documentation	6 years from creation or last effective date, whichever is later
7.3	Accounting of Disclosures	6 years
7.4	Authorization and Consent Records	6 years
7.5	HITECH Documentation	6 years minimum

7.6	Regulatory Correspondence and Enforcement Documentation	6 years minimum or longer if required
7.7	Governance, Audit and Compliance Records	6 years
8.1	AI Governance Documentation	6 years minimum
8.2	AI Training Documentation	6 years from creation, training activity, authorization expiration, or model retirement, whichever is later
8.3	AI Audit Logs and Monitoring Records	6 years minimum
8.4	AI Model Retirement Records	6 years after model retirement
9.2	Raw Audio Recordings	Deleted following successful transcription and validation unless retention is otherwise required
9.2	Audio Access Logs	6 years
9.2	Audio Activity Logs	6 years
9.2	Audio Deletion Logs	6 years
9.2	Voice Consent Records	6 years
9.2	Voice Recording Authorizations	6 years
9.2	Audio Security Reviews	6 years
9.2	Audio Risk Assessments	6 years
9.2	Voice Processing Audit Records	6 years
9.2	Clinical Transcriptions	Same retention as associated clinical record (7 years minimum)
9.2	Behavioral Health Transcriptions	Same retention as associated clinical record
9.2	Wellness Session Transcriptions	Same retention as associated clinical record
9.2	Voice-to-Text Validation Records	6 years
9.2	Voice Processing Incident Reports	6 years
10.2	Daily Backups	90 days
10.2	Weekly Backups	180 days
10.2	Monthly Backup Archives	12 months
10.2	Quarterly Backup Archives	12 months

10.2	Disaster Recovery Archives	12 months
10.2	Recovery Snapshots	90 days
10.2	Immutable Backup Copies	90 days or customer requirement
10.2	Long-Term Archives	Contractual, legal, regulatory, or customer driven
10.4	Recovery Testing Documentation	6 years
10.6	Backup Destruction Records	6 years
11.3	Customer Data Export Availability	Available for request within 30 days following termination
11.4	Production Customer Data	Returned, deleted, anonymized, or otherwise dispositioned within 90 days unless otherwise required
11.8	Destruction Certificates	6 years minimum
12.9	Legal Hold and eDiscovery Records	6 years after legal hold release or matter closure, whichever is later
13.6	Destruction Verification Records	6 years minimum
13.7	Certificates of Destruction	6 years minimum
13.9	Secure Disposal Records	6 years minimum
14.6	Vendor Destruction Attestations	6 years minimum
14.7	Vendor Compliance and Disposition Records	6 years minimum
15.6	Compliance Evidence, Audit Records, Monitoring Records, Legal Hold Records	6 years minimum
18	Glossary	Not applicable
19	Conclusion	Not applicable

Enterprise Retention Summary

7-Year Retention

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

- Messaging Records
- Clinical Transcriptions

6-Year Retention

- HIPAA Documentation
- HITECH Documentation
- Privacy Records
- Consent Records
- Authorization Records
- Disclosure Records
- Security Records
- Audit Logs
- Compliance Records
- AI Governance Records
- Voice Processing Records
- Legal Hold Records
- Vendor Attestations
- Destruction Records

Operational Retention

- Daily Backups: 90 Days
- Weekly Backups: 180 Days
- Monthly Archives: 12 Months
- Disaster Recovery Archives: 12 Months
- Long-Term Archives: Contract / Regulatory Driven

Event-Based Retention

- Raw Audio: Delete after successful transcription and validation
- AI Training Documentation: 6 years after last applicable event
- Legal Hold Records: 6 years after release or matter closure
- BAAs: 6 years after termination
- Customer Data: Return/Delete/Anonymize within 90 days after offboarding unless otherwise required

19. Conclusion

The Cognera Health™ Data Retention, Deletion, and Secure Disposal Policy establishes a comprehensive information lifecycle management and governance framework designed to ensure the secure, compliant, and responsible management of information from creation and collection through retention, archival, preservation, deletion, destruction, and final disposition.

This policy supports alignment with applicable healthcare regulations, privacy laws, cybersecurity standards, information governance practices, and industry-recognized frameworks, including HIPAA, HITECH, HITRUST Common Security Framework (CSF), GDPR, UK GDPR, CCPA/CPRA, ISO/IEC 27001, ISO/IEC 27701, NIST Cybersecurity Framework, NIST SP 800-88 Media Sanitization Guidelines, and other applicable legal, contractual, regulatory, and organizational requirements.

Through documented retention schedules, privacy rights management, legal hold procedures, secure disposal standards, vendor oversight, customer offboarding controls, backup lifecycle management, audit and compliance monitoring, and continuous improvement activities, Cognera Health maintains a risk-based and compliance-driven approach to information governance and records management.

This policy is intended to ensure that information is retained only for legitimate business, clinical, operational, legal, contractual, regulatory, security, and continuity-of-care purposes; protected throughout its lifecycle using appropriate administrative, technical, and organizational safeguards; and securely deleted, destroyed, anonymized, or otherwise dispositioned when no longer required.

By integrating privacy, security, compliance, accountability, information governance, and operational resilience into its information lifecycle management practices, Cognera Health demonstrates its commitment to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), personal information, consumer health data, customer information, and other sensitive information while maintaining regulatory readiness, audit readiness, customer trust, responsible data stewardship, and excellence in healthcare technology operations.

This policy shall be reviewed periodically and updated as necessary to address evolving regulatory requirements, privacy expectations, cybersecurity threats, emerging technologies, industry standards, customer obligations, organizational growth, and continuous improvement opportunities.

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