CONFIDENTIAL

Meridian Health Technologies, Inc.

Information Security Policy

Enterprise Security Program

Document ID	MHT-ISP-2026-001
Version	4.2
Classification	Confidential — Internal Use Only
Effective Date	January 15, 2026
Next Review Date	January 15, 2027
Document Owner	Chief Information Security Officer (CISO)
Approved By	Board of Directors — Security Committee
Distribution	All employees, contractors, and third-party service providers

Document Control

Revision History

Version	Date	Author	Description
1.0	March 10, 2022	David Chen, CISO	Initial policy creation
2.0	September 5, 2022	David Chen, CISO	Added HIPAA and SOC 2 control mappings
3.0	April 18, 2023	Sarah Kim, VP Security	Major revision: cloud security controls, vendor risk management, updated incident response procedures
3.1	November 2, 2023	David Chen, CISO	Updated data classification scheme; added IoT device security provisions
4.0	June 12, 2024	Rachel Torres, CISO	Comprehensive rewrite: AI governance controls, zero-trust architecture requirements, updated regulatory mappings for GDPR Article 25, NIST CSF 2.0
4.1	September 28, 2025	Rachel Torres, CISO	Added remote work security controls; updated encryption standards to FIPS 140-3
4.2	January 15, 2026	Rachel Torres, CISO	Annual review: updated access control procedures, vendor assessment criteria, incident response playbooks, and business continuity provisions

Approval Record

Name / Title	Role	Date	Signature
Rachel Torres, CISSP, CISM Chief Information Security Officer	Document Owner	January 15, 2026	Digitally Signed
Michael Okonkwo Chief Technology Officer	Technical Approver	January 15, 2026	Digitally Signed
Jennifer Walsh, JD, CIPP/US General Counsel & DPO	Legal & Privacy Approver	January 15, 2026	Digitally Signed
Dr. James Liu Chief Executive Officer	Executive Sponsor	January 15, 2026	Digitally Signed
Board Security Committee	Governing Authority	January 15, 2026	Resolution #2026-SEC-004

Related Documents

Document ID	Title	Relationship
MHT-ACP-2026-001	Access Control Policy	Subsidiary policy
MHT-IRP-2026-001	Incident Response Plan	Subsidiary policy
MHT-BCP-2026-001	Business Continuity and Disaster Recovery Plan	Subsidiary policy
MHT-DCP-2026-001	Data Classification and Handling Policy	Subsidiary policy
MHT-VRM-2026-001	Vendor Risk Management Policy	Subsidiary policy
MHT-CMP-2026-001	Change Management Policy	Subsidiary policy
MHT-AUP-2026-001	Acceptable Use Policy	Subsidiary policy
MHT-PNP-2026-001	Privacy Notice and Policy	Subsidiary policy
MHT-RAR-2025-001	Risk Assessment Report (Annual)	Supporting document
MHT-SAR-2025-Q4	Security Awareness Training Report	Supporting document

Table of Contents

1. Executive Summary

Meridian Health Technologies, Inc. (“Meridian Health” or “the Company”) is a healthcare technology company providing cloud-based electronic health record (EHR) management, clinical decision support, and patient engagement platforms to healthcare providers, payers, and life sciences organizations across North America and the European Union.

This Information Security Policy (“Policy”) establishes the framework for protecting the confidentiality, integrity, and availability of information assets owned, controlled, or processed by Meridian Health. It defines the security objectives, organizational responsibilities, risk management approach, and control requirements that govern all aspects of information security across the enterprise.

As a processor and controller of protected health information (PHI), personally identifiable information (PII), and other sensitive data categories, Meridian Health operates under extensive regulatory obligations including but not limited to the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Service Organization Control 2 (SOC 2) Trust Services Criteria, and ISO/IEC 27001:2022.

This Policy serves as the master governance document for the Company’s Information Security Management System (ISMS) and is the root document from which all subsidiary policies, standards, procedures, and guidelines derive their authority.

1.1 Policy Objectives

- Protect the confidentiality, integrity, and availability of all information assets throughout their lifecycle
- Ensure compliance with all applicable laws, regulations, contractual obligations, and industry standards
- Establish clear roles, responsibilities, and accountability for information security at all organizational levels
- Define a risk-based approach to identifying, assessing, treating, and monitoring information security risks
- Provide a foundation for the continuous improvement of the Company’s security posture through measurable objectives and regular review cycles
- Support business operations by enabling secure innovation while maintaining appropriate controls
- Build and maintain trust with customers, partners, regulators, and other stakeholders through demonstrated security maturity

1.2 Scope

This Policy applies to:

- **All personnel:** Full-time and part-time employees, temporary staff, interns, consultants, contractors, and any individual granted access to Meridian Health information systems or data
- **All information assets:** Data in any form (electronic, paper, verbal), information systems, applications, networks, infrastructure, cloud services, mobile devices, IoT devices, and operational technology
- **All locations:** Corporate offices (Boston, MA headquarters; Austin, TX engineering center; London, UK European operations), data center facilities, co-location sites, remote work environments, and any location where Company data is accessed, processed, or stored
- **All third parties:** Vendors, suppliers, partners, and service providers who access, process, store, or transmit Company data or connect to Company networks
- **All cloud environments:** Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and hybrid cloud deployments across Google Cloud Platform, Amazon Web Services, and Microsoft Azure

Exclusions: This Policy does not govern publicly available information that has been formally classified as “Public” through the Company’s data classification process, or information systems that have been formally decommissioned in accordance with the asset disposal procedure.

2. Information Security Governance

Meridian Health maintains a layered governance structure to ensure effective oversight, management, and operational execution of information security across the organization.

2.1 Organizational Structure and Responsibilities

2.1.1 Board of Directors — Security Committee

- Provides executive oversight of the Company's information security program and risk posture
- Reviews and approves the Information Security Policy on an annual basis or following material changes
- Receives quarterly security briefings from the CISO on threat landscape, incident trends, compliance status, and program effectiveness
- Ensures adequate budget and resource allocation for information security initiatives
- Reviews material security incidents and associated remediation actions

2.1.2 Chief Information Security Officer (CISO)

The CISO serves as the senior executive responsible for the design, implementation, and continuous improvement of the Company's information security program. The CISO reports directly to the Chief Technology Officer with a dotted-line reporting relationship to the Board Security Committee.

Responsibilities include:

- Developing, maintaining, and enforcing information security policies, standards, and procedures
- Leading the Security Operations Center (SOC) and incident response function
- Managing the enterprise risk assessment program and maintaining the risk register
- Overseeing security architecture reviews for all new systems and material changes
- Directing the security awareness and training program
- Serving as the primary liaison with external auditors, regulators, and law enforcement on security matters
- Reporting on security metrics, key risk indicators (KRIs), and program effectiveness to executive leadership and the Board

2.1.3 Data Protection Officer (DPO)

The General Counsel serves as the designated Data Protection Officer in accordance with GDPR Article 37. The DPO operates independently on data protection matters and reports directly to the Board on privacy-related issues.

- Monitors compliance with GDPR, HIPAA Privacy Rule, CCPA, and other applicable privacy regulations
- Conducts and oversees Data Protection Impact Assessments (DPIAs) for high-risk processing activities
- Serves as the point of contact for data subjects, supervisory authorities, and privacy regulators
- Advises on privacy-by-design and privacy-by-default requirements for new products and services

2.1.4 Information Security Team

The Information Security team, led by the CISO, comprises the following functional areas:

- **Security Engineering:** Designs, implements, and maintains security infrastructure, tools, and controls
- **Security Operations (SOC):** Monitors security events, manages SIEM, conducts threat hunting, and coordinates incident response
- **Governance, Risk & Compliance (GRC):** Manages policy framework, risk assessments, audit coordination, and regulatory compliance
- **Application Security:** Conducts code reviews, penetration testing, and vulnerability management for software products
- **Identity & Access Management (IAM):** Administers access controls, authentication systems, and privilege management

2.1.5 Department Managers and System Owners

- Ensure personnel within their departments comply with this Policy and all subsidiary security policies
- Identify and classify information assets under their ownership in accordance with the Data Classification Policy
- Participate in risk assessments for systems and processes under their responsibility
- Approve access requests for systems they own, ensuring the principle of least privilege is maintained
- Report security incidents, vulnerabilities, and policy violations promptly through established channels

2.1.6 All Personnel

Every individual with access to Meridian Health information systems or data is personally responsible for:

- Reading, understanding, and complying with this Policy and all applicable subsidiary policies

- Completing mandatory security awareness training within 30 days of hire and annually thereafter
- Protecting Company credentials and not sharing passwords or access tokens with any other individual
- Reporting suspected security incidents, vulnerabilities, or policy violations immediately to the Security Operations Center via security@meridianhealth.com or the internal reporting portal
- Safeguarding physical and electronic information assets in their possession or under their control

2.2 Policy Framework

The Company's information security documentation follows a four-tier hierarchy:

- **Tier 1 — Policies:** High-level statements of management intent and direction. This Information Security Policy is the Tier 1 document from which all other documents derive authority. Approved by the Board Security Committee.
- **Tier 2 — Standards:** Mandatory requirements that specify the minimum security controls and configurations. Examples include encryption standards, password complexity requirements, and network segmentation standards. Approved by the CISO.
- **Tier 3 — Procedures:** Step-by-step instructions for implementing policies and standards. Examples include the incident response procedure, access provisioning procedure, and change management procedure. Approved by functional area leads.
- **Tier 4 — Guidelines:** Recommended best practices and advisory information. Guidelines are not mandatory but represent the Company's recommended approach. Published by the Information Security team.

2.3 Policy Review and Maintenance

This Policy shall be reviewed and, if necessary, updated:

- At least annually, with the next scheduled review by January 15, 2027
- Following any material security incident that exposes a control deficiency
- Upon significant changes to the regulatory landscape, business operations, technology environment, or threat landscape
- When directed by the Board Security Committee, executive leadership, or external auditors

All policy changes must be approved through the established governance process and communicated to all personnel within 30 days of approval.

3. Risk Management

Meridian Health adopts a risk-based approach to information security, aligned with ISO 31000:2018, NIST SP 800-30, and the NIST Cybersecurity Framework 2.0. Risk management is integrated into strategic planning, system development, change management, and daily operations.

3.1 Risk Assessment Methodology

The Company conducts comprehensive risk assessments using the following methodology:

3.1.1 Asset Identification

- Maintain an inventory of all information assets, including data repositories, applications, infrastructure components, cloud services, and intellectual property
- Classify each asset according to the Data Classification Policy (Public, Internal, Confidential, Restricted)
- Assign ownership to a named individual or role for each asset
- Document the business value, criticality, and sensitivity of each asset

3.1.2 Threat and Vulnerability Assessment

- Identify threats relevant to each asset category, including cyber threats, physical threats, insider threats, supply chain threats, and natural disasters
- Conduct vulnerability assessments on a continuous basis using automated scanning tools
- Perform annual penetration testing of external-facing systems and critical internal systems by qualified third-party assessors
- Monitor threat intelligence feeds and advisories from CISA, MITRE ATT&CK, and industry ISACs

3.1.3 Risk Evaluation

Risks are evaluated using a qualitative 5x5 risk matrix:

Impact \ Likelihood	Rare	Unlikely	Possible	Likely
Catastrophic	Medium	High	Critical	Critical
Major	Low	Medium	High	Critical
Moderate	Low	Medium	Medium	High

Impact \ Likelihood	Rare	Unlikely	Possible	Likely
Minor	Low	Low	Low	Medium
Insignificant	Low	Low	Low	Low

3.1.4 Risk Treatment

For each identified risk exceeding the Company's risk appetite, one of the following treatment strategies shall be selected and documented:

- **Mitigate:** Implement controls to reduce the likelihood or impact of the risk to an acceptable level
- **Transfer:** Share the risk with a third party through insurance, contractual arrangements, or outsourcing with appropriate controls
- **Accept:** Formally accept the residual risk with documented approval from the appropriate risk owner. Risks rated Critical or High require CISO approval; risks rated Medium require department manager approval
- **Avoid:** Eliminate the risk by discontinuing the activity that gives rise to the risk

3.2 Risk Register

The CISO maintains an enterprise risk register documenting all identified risks, their current assessment, treatment plans, assigned owners, and target remediation dates. The risk register is reviewed:

- Monthly by the Information Security team
- Quarterly by executive leadership
- Annually by the Board Security Committee

3.3 Risk Appetite Statement

Meridian Health has a low appetite for risks that could compromise the confidentiality of patient health information, personally identifiable information, or other regulated data. The Company has moderate appetite for operational risks that do not directly impact data confidentiality and can be managed through standard business continuity measures.

The following risk tolerance thresholds apply:

- **Critical risks:** Must be treated immediately. No Critical risks may be accepted without Board Security Committee approval
- **High risks:** Must have active treatment plans with target remediation within 30 days
- **Medium risks:** Must have documented treatment plans with target remediation within 90 days
- **Low risks:** Tracked and reviewed during regular assessment cycles

4. Data Classification and Protection

Meridian Health classifies all information assets based on their sensitivity, regulatory requirements, and business impact. This classification determines the minimum set of security controls applied throughout the data lifecycle.

4.1 Classification Levels

Level	Definition	Examples	Handling Requirements
Restricted	Highest sensitivity. Unauthorized disclosure would cause severe harm to individuals or the Company. Subject to specific regulatory requirements.	Protected Health Information (PHI), payment card data (PCI), Social Security numbers, biometric data, encryption keys, system credentials	Encrypted at rest (AES-256) and in transit (TLS 1.2+). Access on strict need-to-know basis. Multi-factor authentication required. Detailed access logging. No storage on personal devices.
Confidential	Sensitive business information. Unauthorized disclosure would cause significant harm.	Employee records, financial data, source code, customer contracts, strategic plans, security configurations, audit reports	Encrypted at rest and in transit. Access limited to authorized personnel. NDA required for third-party access. Logical access controls enforced.
Internal	General business information not intended for public release. Unauthorized disclosure would cause limited harm.	Internal communications, meeting notes, project documentation, organizational charts, training materials	Standard access controls. Not to be shared externally without authorization. Reasonable precautions against unauthorized disclosure.
Public	Information approved for public distribution. No harm from disclosure.	Published marketing materials, press releases, public-facing website content, open-source code	No special handling requirements. Must be explicitly classified as Public through formal approval.

4.2 Data Retention and Disposal

Information assets shall be retained in accordance with applicable legal, regulatory, and business requirements. The following minimum retention periods apply:

- **Protected Health Information (PHI):** Six (6) years from the date of creation or the date when last in effect, whichever is later, in accordance with HIPAA regulations
- **Financial records:** Seven (7) years in accordance with SOX requirements and IRS guidelines
- **Employee records:** Duration of employment plus seven (7) years
- **Security logs and audit trails:** Minimum one (1) year online, three (3) years in archive
- **Customer contract data:** Duration of the contract plus five (5) years
- **GDPR personal data:** Only for as long as necessary for the specified processing purpose. Data subjects may request deletion in accordance with applicable regulations.

Secure Disposal: When information assets reach the end of their retention period or are no longer required, they must be disposed of securely using methods appropriate to the classification level. Restricted and Confidential data must be destroyed using NIST SP 800-88 compliant methods. Certificates of destruction must be obtained and retained for media containing Restricted data.

5. Access Control

Meridian Health implements access controls based on the principles of least privilege, need-to-know, and separation of duties. Access to all information systems and data is granted only to authorized personnel who require such access to perform their assigned duties.

5.1 Access Control Principles

- **Least privilege:** Users are granted the minimum level of access necessary to perform their job functions. Elevated privileges are granted only when justified by specific business requirements and are subject to enhanced monitoring
- **Need-to-know:** Access to Restricted and Confidential data is limited to individuals who have a demonstrated and documented business need
- **Separation of duties:** Critical functions are divided among different individuals to reduce the risk of fraud, error, or unauthorized activity. No single individual may approve their own access requests, deploy their own code changes to production, or simultaneously hold conflicting roles
- **Defense in depth:** Multiple layers of access controls are implemented to provide redundant protection against unauthorized access

5.2 User Authentication

5.2.1 Password Requirements

All password-based authentication must meet the following minimum requirements:

- Minimum length: 14 characters for standard accounts, 20 characters for privileged accounts
- Must contain a combination of uppercase letters, lowercase letters, numbers, and special characters
- Passwords must not contain the user’s name, username, or commonly used password patterns
- Password history: users may not reuse any of their previous 12 passwords
- Maximum password age: 90 days for standard accounts, 60 days for privileged accounts
- Account lockout after 5 consecutive failed authentication attempts; lockout duration of 30 minutes or until administratively reset

5.2.2 Multi-Factor Authentication (MFA)

Multi-factor authentication is required for:

- All remote access to Company systems and networks, including VPN connections
- All access to cloud management consoles (GCP, AWS, Azure)

- All privileged or administrative access to any system
- Access to systems containing Restricted or Confidential data
- Email access from non-Company-managed devices

Approved MFA methods include hardware security keys (FIDO2/WebAuthn), authenticator applications (TOTP), and push notifications from approved providers. SMS-based authentication is not approved for new implementations and is being phased out from existing systems by Q3 2026.

5.3 Access Provisioning and Deprovisioning

5.3.1 Access Request and Approval

All access requests must be submitted through the Company's identity management system and must include:

- The specific systems, applications, or data repositories for which access is requested
- The level of access required (read, write, admin) and business justification
- The expected duration of access (permanent or time-limited)

Access must be approved by the system owner or their designated delegate before provisioning. Requests for privileged access require additional approval from the CISO or their delegate.

5.3.2 Access Reviews

Access rights are reviewed periodically to ensure they remain appropriate and aligned with current job responsibilities:

- **Privileged accounts:** Reviewed quarterly by the IAM team with system owner validation
- **Standard user accounts:** Reviewed periodically by department managers to confirm continued need
- **Service accounts:** Reviewed semi-annually by the Security Engineering team
- **Third-party access:** Reviewed upon contract renewal or annually, whichever is sooner

Note: *Access review findings must be remediated within 14 days of the review completion. Access that cannot be justified is revoked immediately.*

5.3.3 Termination and Role Change

Upon notification of employee termination:

- All access must be revoked within 4 hours of the effective termination time for voluntary departures
- All access must be revoked immediately (within 1 hour) for involuntary terminations

- Company-issued devices must be returned and securely wiped within 5 business days
- Active sessions must be terminated and authentication tokens invalidated

Upon role change or transfer, access rights are reviewed by the new manager and adjusted to reflect the new role's requirements. Previous access that is no longer needed must be revoked within 5 business days.

5.4 Privileged Access Management

Privileged accounts (root, administrator, database admin, cloud admin) are subject to enhanced controls:

- Privileged access is managed through a Privileged Access Management (PAM) solution with session recording
- Standing privileged access is minimized; just-in-time (JIT) access is used wherever technically feasible
- All privileged sessions are logged and monitored in real-time by the SOC
- Shared accounts are prohibited; each privileged user must have a unique, attributable account
- Emergency (break-glass) accounts exist for system recovery scenarios; their use triggers immediate alerts and requires post-use review and justification

6. Network Security

Meridian Health implements a defense-in-depth approach to network security, employing multiple layers of controls to protect information assets from unauthorized access, misuse, and disruption.

6.1 Network Architecture

- All networks are segmented based on trust level, data sensitivity, and functional purpose using VLANs, firewalls, and cloud VPC configurations
- Production environments are logically isolated from development, testing, and corporate environments
- A demilitarized zone (DMZ) architecture is maintained for all internet-facing services
- Zero-trust network principles are applied: no implicit trust is granted based on network location; all access requires authentication and authorization regardless of network segment

6.2 Firewall and Perimeter Controls

- Next-generation firewalls are deployed at all network boundaries with application-layer inspection enabled
- Default-deny rules are implemented on all firewalls; only explicitly authorized traffic is permitted
- Firewall rules are reviewed quarterly and after any significant network change
- Web Application Firewalls (WAF) are deployed in front of all public-facing web applications
- Intrusion Detection and Prevention Systems (IDS/IPS) monitor all network traffic at critical junctions

6.3 Wireless Network Security

- Corporate wireless networks use WPA3-Enterprise with 802.1X authentication against the Company's directory service
- Guest wireless networks are isolated from corporate networks and provide internet access only
- Rogue wireless access point detection is enabled across all office locations
- IoT devices are placed on dedicated, isolated network segments with restricted communication paths

6.4 Remote Access and VPN

All remote access to Company networks and systems must be conducted through approved channels:

- Always-on VPN is required for Company-managed devices connecting from external networks
- Split tunneling is disabled; all traffic routes through the Company's security stack
- VPN connections require multi-factor authentication
- Remote access sessions are subject to inactivity timeout of 15 minutes for systems accessing Restricted data, 30 minutes for all other systems
- BYOD access to corporate email and collaboration tools is permitted only through approved mobile device management (MDM) enrolled devices

6.5 Encryption in Transit

All data transmitted over networks, including internal networks, must be encrypted using approved protocols:

- TLS 1.2 or higher for all web-based communications; TLS 1.3 preferred
- SSH version 2 for all administrative access to servers and infrastructure
- IPsec or WireGuard for site-to-site VPN connections
- TLS 1.0 and 1.1 are prohibited and must be disabled on all systems
- Self-signed certificates are prohibited in production environments; all certificates must be issued by approved Certificate Authorities

7. Endpoint and Device Security

7.1 Company-Managed Devices

All Company-issued endpoints (laptops, desktops, mobile devices) must meet the following security baseline:

- Enrolled in the Company's endpoint management platform (MDM/UEM)
- Full disk encryption enabled (BitLocker for Windows, FileVault for macOS)
- Endpoint Detection and Response (EDR) agent installed and active
- Host-based firewall enabled and configured to Company standards
- Automatic operating system and application patching enabled; critical patches applied within 72 hours of release, high-severity patches within 7 days
- Local administrator rights are not granted to standard users; elevation requires PAM approval
- Screen lock activates after 5 minutes of inactivity

7.2 Mobile Device Security

- Company data may only be accessed from mobile devices enrolled in the approved MDM solution
- Devices must have a PIN/biometric lock enabled with a minimum 6-digit PIN
- Remote wipe capability must be enabled and testable
- Jailbroken or rooted devices are prohibited from accessing Company systems
- Company data is stored in managed containers separate from personal data (COPE and BYOD)

7.3 Removable Media

The use of removable media (USB drives, external hard drives, SD cards) is restricted:

- USB mass storage devices are blocked by default on all Company-managed endpoints via endpoint management policy
- Exceptions require written approval from the CISO and are limited in scope and duration
- Approved removable media must be encrypted and tracked in the asset inventory
- Removable media containing Restricted data must be stored in physically secure locations when not in use

8. Cryptographic Controls

Meridian Health employs cryptographic controls to protect the confidentiality and integrity of sensitive information in accordance with NIST SP 800-175B and FIPS 140-3 requirements.

8.1 Encryption Standards

Context	Minimum Standard	Implementation
Data at rest — Restricted	AES-256-GCM	Database-level encryption (Google Cloud KMS, AWS KMS), full disk encryption on all endpoints and servers
Data at rest — Confidential	AES-256	Disk-level encryption with platform-managed keys or customer-managed keys where contractually required
Data in transit — External	TLS 1.2+ (TLS 1.3 preferred)	All external-facing services; HSTS enabled with minimum 1-year max-age
Data in transit — Internal	TLS 1.2+	Service mesh mTLS for microservices; encrypted database connections
Backups	AES-256	All backup data encrypted before transfer and at rest in storage
Key exchange	RSA 2048+ or ECDHE P-256+	Forward secrecy required for all TLS sessions
Hashing (passwords)	bcrypt (cost factor 12+) or Argon2id	Salted and stretched; SHA-256 for non-authentication use cases
Digital signatures	RSA 2048+ or ECDSA P-256+	Code signing, document signing, API authentication

8.2 Key Management

- Encryption keys are generated using cryptographically secure random number generators
- Key management is performed using hardware security modules (HSMs) or cloud KMS services validated to FIPS 140-3 Level 2 or higher
- Encryption keys are rotated annually at minimum, or immediately if compromise is suspected
- Key access is restricted to the minimum number of authorized personnel required for operational needs
- Key escrow and recovery procedures are documented and tested annually

- Retired keys are archived securely for the duration of the data they protect, then destroyed

8.3 Certificate Management

- All TLS certificates are managed through an automated certificate lifecycle management platform
- Certificate expiration is monitored with alerts generated 30 days prior to expiration
- Wildcard certificates are permitted only for non-production environments; production services use individual certificates
- Certificate transparency logging is enabled for all public-facing certificates

9. Application Security

Meridian Health integrates security throughout the software development lifecycle (SDLC) to ensure that applications are designed, developed, tested, and deployed with appropriate security controls.

9.1 Secure Development Lifecycle

- **Security requirements:** Security and privacy requirements are defined during the design phase for all new applications and significant changes, including threat modeling using STRIDE methodology
- **Secure coding standards:** Developers follow OWASP Secure Coding Practices and language-specific security guidelines. Training on secure coding is mandatory for all developers annually
- **Code review:** All production code changes require peer review by at least one reviewer with security awareness training. Security-sensitive changes require review by the Application Security team
- **Static analysis (SAST):** Automated static analysis scanning is integrated into the CI/CD pipeline and runs on every commit. Critical and high findings must be resolved before merge
- **Dynamic analysis (DAST):** Dynamic application security testing is performed on staging environments before production deployment
- **Software Composition Analysis (SCA):** Third-party libraries and dependencies are scanned for known vulnerabilities. Components with critical CVEs must be updated or replaced within 48 hours

9.2 Vulnerability Management

Vulnerabilities are triaged and remediated according to the following SLAs:

Severity	CVSS Score	Remediation SLA	Escalation
Critical	9.0 – 10.0	24 hours	CISO + CTO notified immediately
High	7.0 – 8.9	7 days	Security Engineering lead
Medium	4.0 – 6.9	30 days	System owner
Low	0.1 – 3.9	90 days	Tracked in vulnerability management system

9.3 Penetration Testing

- External penetration testing is conducted annually by qualified third-party assessors
- Internal penetration testing and red team exercises are conducted semi-annually
- Penetration testing scope includes web applications, APIs, mobile applications, network infrastructure, and cloud configurations
- All critical and high findings from penetration tests must be remediated within the SLAs defined above
- Remediation is verified through re-testing before findings are closed

9.4 API Security

- All APIs require authentication; unauthenticated APIs are prohibited in production
- API rate limiting is implemented to prevent abuse and denial-of-service attacks
- API input validation is enforced on all endpoints; all input is treated as untrusted
- API keys and tokens are rotated at minimum every 90 days
- API access logs are retained and monitored by the SOC

10. Cloud Security

Meridian Health operates a multi-cloud environment spanning Google Cloud Platform (primary), Amazon Web Services (secondary), and Microsoft Azure (specific workloads). Cloud security controls are implemented in accordance with the shared responsibility model.

10.1 Cloud Governance

- All cloud resources are provisioned through Infrastructure-as-Code (IaC) templates that enforce security baselines
- Cloud configurations are continuously monitored against CIS Benchmarks for GCP, AWS, and Azure
- Cloud Security Posture Management (CSPM) tools alert on configuration drift and non-compliant resources
- Landing zone architectures are maintained for each cloud provider with pre-approved security configurations

10.2 Identity and Access in Cloud

- Cloud IAM follows the principle of least privilege; broad-scope roles (e.g., Owner, Admin) are restricted to break-glass accounts
- Service accounts use workload identity federation; long-lived service account keys are prohibited
- Cloud resource access is logged and monitored through cloud-native audit logging (Cloud Audit Logs, CloudTrail, Azure Activity Logs)

10.3 Data Residency and Sovereignty

Customer data is stored in geographic regions specified in customer contracts and in accordance with applicable data sovereignty laws:

- US customer data: processed and stored in US regions (us-central1, us-east1)
- EU customer data: processed and stored in EU regions (europe-west1, europe-west3) in accordance with GDPR data transfer requirements
- Data is not transferred across jurisdictional boundaries without appropriate legal mechanisms (Standard Contractual Clauses, adequacy decisions, or binding corporate rules)

11. Security Incident Management

Meridian Health maintains a comprehensive incident response capability to detect, respond to, contain, eradicate, and recover from security incidents in a timely and effective manner.

11.1 Incident Classification

Security incidents are classified based on severity to ensure appropriate response:

Severity	Definition	Examples	Response Time
SEV-1 (Critical)	Confirmed breach of Restricted data; material impact to business operations or regulatory obligations	Ransomware affecting production systems; confirmed PHI data exfiltration; complete loss of critical infrastructure	Immediate response; CISO and executive leadership notified within 15 minutes
SEV-2 (High)	Significant security event with potential for data loss or material business impact	Unauthorized access to Confidential systems; active exploitation of critical vulnerability; insider threat indicators	Response within 1 hour; CISO notified within 30 minutes
SEV-3 (Medium)	Security event requiring investigation; limited immediate impact	Malware detected and contained on single endpoint; phishing campaign targeting employees; failed intrusion attempt	Response within 4 hours during business hours
SEV-4 (Low)	Minor security event; informational	Policy violation; single failed login from unusual location; minor misconfiguration detected	Response within 24 hours

11.2 Incident Response Phases

11.2.1 Detection and Reporting

Security incidents may be detected through:

- SOC monitoring and SIEM alerting (24/7 coverage)
- Endpoint detection and response (EDR) alerts
- Employee reports via security@meridianhealth.com or the internal reporting portal
- Automated vulnerability scanning and configuration monitoring
- External reports from customers, partners, or security researchers through the responsible disclosure program

All employees must report suspected security incidents immediately upon discovery. There is no penalty for good-faith reporting of potential incidents.

11.2.2 Containment

The incident response team takes immediate action to contain the incident and prevent further damage:

- Isolate affected systems from the network while preserving forensic evidence
- Disable compromised accounts and revoke associated access tokens
- Block malicious IP addresses, domains, or communication channels
- Implement temporary compensating controls as needed

11.2.3 Eradication and Recovery

- Remove the root cause of the incident (malware, unauthorized access, vulnerability)
- Restore affected systems from known-good backups after confirming integrity
- Apply patches or configuration changes to prevent recurrence
- Verify system integrity before returning to production operations

11.2.4 Post-Incident Activities

- Conduct a post-incident review (blameless post-mortem) within 5 business days of incident closure
- Document lessons learned and corrective actions in the incident management system
- Update security controls, procedures, and detection capabilities based on findings
- Provide updated threat intelligence to the SOC for integration into monitoring

11.3 Breach Notification

Meridian Health will notify affected parties of confirmed data breaches in accordance with applicable legal and regulatory requirements:

- **HIPAA:** Affected individuals and the Department of Health and Human Services (HHS) will be notified without unreasonable delay. For breaches affecting 500 or more individuals, notification will be provided to prominent media outlets serving the affected area
- **GDPR:** The relevant supervisory authority will be notified within 72 hours of becoming aware of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals. Affected data subjects will be notified without undue delay when the breach is likely to result in a high risk

- **State breach notification laws:** Notifications will be made in accordance with the requirements of each applicable state. The legal department maintains a matrix of state-specific notification requirements and timelines
- **Contractual obligations:** Customers and partners will be notified in accordance with the terms of applicable contracts and service level agreements

Note: *The DPO and General Counsel must be consulted before any external breach notification is issued.*

12. Physical and Environmental Security

12.1 Office Security

- All Company office locations implement badge-based physical access control systems
- Visitor access requires sign-in, photo identification, escort by an employee, and a visitor badge that must be visibly displayed
- Security cameras with 90-day retention monitor entry points, server rooms, and common areas
- Clean desk policy is enforced: sensitive documents and removable media must be secured at end of day

12.2 Data Center and Server Room Security

- Physical access to server rooms and network closets is restricted to authorized personnel with documented business need
- Server rooms employ multi-factor physical access controls (badge + biometric)
- Environmental controls include redundant HVAC, fire suppression (FM-200 or equivalent), water leak detection, and uninterruptible power supplies
- Third-party data centers and co-location facilities are assessed annually against SOC 2 Type II and relevant physical security standards

12.3 Equipment Disposal

All equipment containing data storage media must be sanitized or destroyed before disposal or reuse:

- Hard drives and solid-state drives are sanitized using NIST SP 800-88 methods (Clear, Purge, or Destroy based on data classification)
- Physical destruction is required for media that previously stored Restricted data
- Certificates of destruction are obtained and retained for all sanitized or destroyed media
- Asset disposal is tracked in the asset management system with chain-of-custody documentation

13. Security Awareness and Training

Meridian Health maintains a comprehensive security awareness and training program to ensure all personnel understand their responsibilities for protecting information assets.

13.1 Training Requirements

Training Type	Audience	Frequency	Delivery Method
General Security Awareness	All personnel	Within 30 days of hire; annually thereafter	Online interactive course with assessment; minimum 80% passing score
HIPAA Privacy and Security	All personnel with access to PHI	Within 30 days of hire; annually thereafter	Online course with scenario-based exercises
Phishing Simulation	All personnel with email access	Monthly	Simulated phishing campaigns with immediate educational feedback
Secure Coding	Software developers	Annually	Instructor-led or online course covering OWASP Top 10 and language-specific security
Incident Response	Incident response team	Quarterly	Tabletop exercises and live-fire drills
Privileged Access	Administrators with elevated access	Semi-annually	Focused training on PAM procedures, logging, and accountability
Executive Security Briefing	C-suite and Board members	Quarterly	CISO-led briefing on threat landscape, risk posture, and incidents

13.2 Training Effectiveness

- Training completion rates are tracked and reported monthly; target is 95% compliance within the required timeframe
- Phishing simulation click rates are tracked as a KRI; the organizational target is below 5%
- Personnel who fail phishing simulations receive immediate supplemental training and are re-tested within 30 days

- Annual training content is updated to reflect current threat landscape, recent incidents, and emerging attack techniques

14. Business Continuity and Disaster Recovery

Meridian Health maintains business continuity and disaster recovery capabilities to ensure the resilience of critical business operations and the rapid recovery of information systems following disruptive events.

14.1 Business Impact Analysis

A Business Impact Analysis (BIA) is conducted annually to identify critical business processes, quantify the impact of disruptions, and establish recovery priorities:

- Maximum Tolerable Downtime (MTD) is established for each critical business process
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are defined for all critical systems
- Dependencies between systems, processes, and third parties are mapped and documented

14.2 Recovery Objectives

System Category	RTO	RPO	Strategy
Patient-facing clinical systems	4 hours	1 hour	Active-active multi-region deployment with automatic failover
Internal business applications	24 hours	4 hours	Warm standby in secondary region with automated recovery
Development and test environments	72 hours	24 hours	Infrastructure-as-Code rebuild from templates and backups
Corporate systems (email, collaboration)	8 hours	4 hours	SaaS provider SLA + backup configuration

14.3 Backup and Recovery

- All production data is backed up daily with incremental backups throughout the day
- Backups are encrypted using AES-256 before transfer and at rest
- Backup copies are stored in a geographically separate location from the primary data
- Backup integrity is verified through automated validation checks after each backup job
- Full restoration tests are conducted quarterly for critical systems and annually for all systems
- Backup retention follows the data retention schedule defined in Section 4.2

14.4 Plan Testing

Business continuity and disaster recovery plans are tested through the following schedule:

- **Tabletop exercises:** Semi-annually, involving all stakeholders in the BC/DR plan
- **Technical failover testing:** Quarterly for Tier 1 (patient-facing) systems
- **Full-scale DR exercise:** Annually, simulating a complete primary region failure with actual failover to the secondary region
- **Communication tree test:** Quarterly, verifying contact information and notification procedures

Test results are documented, including any failures or gaps identified. Remediation plans are developed for all identified deficiencies and tracked to completion.

15. Third-Party and Vendor Risk Management

Meridian Health requires that all third-party service providers who access, process, store, or transmit Company data, or who connect to Company networks, are assessed for security risk and managed throughout the engagement lifecycle.

15.1 Vendor Assessment

Third parties are assessed prior to engagement and periodically thereafter based on their risk tier:

Risk Tier	Criteria	Assessment Requirements	Review Frequency
Critical	Processes or stores Restricted data (PHI, PCI); direct access to production systems; single point of failure	Full security assessment questionnaire (SIG), SOC 2 Type II report review, penetration test results, insurance verification, on-site assessment (if applicable)	Annually
High	Processes or stores Confidential data; network connectivity; significant business dependency	Security questionnaire, SOC 2 report or ISO 27001 certification review, insurance verification	Annually
Medium	Limited data access (Internal classification); no network connectivity; substitutable service	Abbreviated security questionnaire, privacy policy review	Every two years
Low	No data access; no network connectivity; commodity service	Basic due diligence (business verification, reputation check)	At renewal

15.2 Contractual Requirements

All third-party agreements involving access to Company data must include:

- Data protection and confidentiality obligations
- Security requirements aligned with the data classification level
- Breach notification requirements (notification within 24 hours of discovery for Critical-tier vendors)
- Right to audit or request evidence of security controls
- Data return and secure destruction obligations upon contract termination
- Subprocessor management requirements (for GDPR compliance)

- Business Associate Agreement (for HIPAA-covered data)

15.3 Ongoing Monitoring

- Continuous monitoring of critical vendors using third-party risk intelligence services
- Review of vendor security incidents and their potential impact on Company data
- Periodic reassessment based on the risk tier schedule above
- Immediate reassessment triggered by any vendor security incident affecting Company data

16. Regulatory Compliance

Meridian Health operates under multiple regulatory frameworks. This section maps the Company's security program to key regulatory and industry requirements.

16.1 Regulatory Framework Mapping

Framework	Applicability	Key Requirements Addressed	Audit Cycle
HIPAA	Processing of Protected Health Information for healthcare customers	Administrative, physical, and technical safeguards; breach notification; Business Associate Agreements	Annual risk assessment; SOC 2 + HITRUST serves as supporting evidence
GDPR	Processing of personal data of EU residents (London office, EU customers)	Lawful processing basis; data subject rights; Data Protection Impact Assessments; cross-border transfer mechanisms; breach notification (72 hours)	Annual DPA review; supervisory authority engagement as needed
SOC 2 Type II	Service organization providing cloud-based services to customers	Trust Services Criteria: Security, Availability, Confidentiality, Processing Integrity, Privacy	Annual audit by independent CPA firm
ISO 27001:2022	ISMS certification for global operations	Annex A controls; Statement of Applicability; continuous improvement	Annual surveillance audit; recertification every 3 years
PCI DSS 4.0	Processing of payment card data for billing operations	12 requirement domains including network security, access control, monitoring, and testing	Annual SAQ-D or QSA audit based on transaction volume
CCPA / CPRA	Processing personal information of California residents	Consumer rights (access, deletion, opt-out); reasonable security measures	Annual review of practices and consumer rights fulfillment
NIST CSF 2.0	Voluntary framework adopted as security program baseline	Six functions: Govern, Identify, Protect, Detect, Respond, Recover	Annual self-assessment; mapped to SOC 2 and ISO 27001 controls

16.2 Internal Audit

- The GRC team conducts an annual internal audit of information security controls aligned with ISO 27001 and SOC 2 requirements
- Internal audit findings are reported to the CISO and tracked in the risk register
- Critical and high findings must be remediated within the timelines defined in Section 3.3
- Internal audit reports are provided to the Board Security Committee

16.3 External Audit

- SOC 2 Type II audit is conducted annually by an independent CPA firm
- ISO 27001 surveillance audits are conducted annually with recertification every three years
- The Company cooperates fully with regulatory examinations and audits
- External audit findings are entered into the risk register and remediated according to defined SLAs

17. Security Monitoring and Logging

Meridian Health implements comprehensive monitoring and logging to detect, investigate, and respond to security events across the environment.

17.1 Logging Requirements

The following events must be logged for all information systems:

- Authentication events (successful and failed login attempts)
- Authorization events (access granted, denied, or escalated)
- Administrative actions (user creation, modification, deletion, privilege changes)
- System events (startup, shutdown, configuration changes, errors)
- Data access events for Restricted and Confidential data
- Network events (firewall permit/deny, VPN connections, DNS queries)
- Application events (API calls, data exports, file uploads)

17.2 Log Management

- All logs are forwarded to the centralized SIEM platform in near real-time
- Logs are retained for a minimum of one (1) year online and three (3) years in archival storage
- Log integrity is protected through write-once storage and cryptographic hashing
- Access to raw log data is restricted to SOC analysts and authorized investigators
- Log sources are inventoried and monitored; missing log sources trigger investigation

17.3 Security Operations Center (SOC)

- The SOC provides 24/7 monitoring coverage for security events
- Automated correlation rules and machine learning models identify suspicious patterns and anomalies
- SOC analysts triage alerts based on severity and potential impact
- Escalation procedures are defined for each alert category with clear ownership
- SOC metrics (mean time to detect, mean time to respond, false positive rate) are tracked and reported monthly

18. Change Management

All changes to production information systems, infrastructure, and configurations are managed through a formal change management process to minimize the risk of unintended disruptions and security vulnerabilities.

18.1 Change Categories

- **Standard changes:** Pre-approved, low-risk changes that follow established procedures (e.g., routine patching, approved software deployments through CI/CD pipelines)
- **Normal changes:** Changes requiring Change Advisory Board (CAB) review and approval before implementation
- **Emergency changes:** Changes required to address an immediate security threat or critical outage. May be implemented with expedited approval from the CISO and on-call manager, with full documentation completed within 48 hours

18.2 Change Approval

- All normal changes require a documented change request including description, risk assessment, rollback plan, and testing evidence
- The Change Advisory Board meets weekly to review pending changes
- Changes affecting security controls, network architecture, or Restricted data systems require CISO approval
- Separation of duties is enforced: the person requesting a change may not approve it, and the person who develops a change may not deploy it to production

18.3 Post-Implementation Review

- All changes are verified post-implementation to confirm expected outcomes and the absence of adverse effects
- Failed or rolled-back changes are documented with root cause analysis
- Unauthorized changes detected through configuration monitoring are investigated as potential security incidents

19. Acceptable Use

This section establishes the expectations for acceptable use of Meridian Health information systems, networks, and data by all personnel.

19.1 General Expectations

- Company information systems are provided for business purposes. Limited personal use is permitted provided it does not interfere with job performance, consume excessive resources, or create security risks
- Users must not attempt to circumvent security controls, access systems beyond their authorization, or probe systems for vulnerabilities without explicit written authorization from the CISO
- Users must not install unauthorized software on Company-managed devices
- Users must not store Restricted or Confidential data on personal devices, personal cloud storage, or unauthorized services

19.2 Prohibited Activities

The following activities are strictly prohibited:

- Sharing Company credentials with any other individual, including IT support staff
- Using Company systems to access, store, or distribute illegal, offensive, or inappropriate content
- Connecting unauthorized devices to the Company network
- Disabling or circumventing endpoint security controls (EDR, disk encryption, firewall)
- Exfiltrating Company data through unauthorized channels (personal email, file sharing, printing)
- Using Company systems for cryptocurrency mining, unauthorized commercial activities, or political campaigning

19.3 Monitoring Notice

Meridian Health reserves the right to monitor, access, and review all data stored on or transmitted through Company systems and networks. Users should have no expectation of privacy when using Company information systems. Monitoring is conducted in accordance with applicable laws and regulations, including employee notification requirements.

20. Artificial Intelligence Governance

Meridian Health recognizes the growing use of artificial intelligence and machine learning technologies within its products and operations. This section establishes governance requirements for the responsible development and use of AI systems.

20.1 AI Risk Assessment

- All AI/ML systems must undergo a risk assessment before deployment, evaluating potential impacts on patient safety, data privacy, fairness, and transparency
- AI systems that influence clinical decisions are classified as high-risk and require additional validation, testing, and monitoring
- Bias testing must be conducted on training data and model outputs, with documented results and remediation of identified biases

20.2 AI Data Governance

- Training data must be sourced, processed, and retained in accordance with the Data Classification Policy and applicable privacy regulations
- Patient data used for AI/ML training must be de-identified in accordance with HIPAA Safe Harbor or Expert Determination methods
- Data lineage must be documented for all AI/ML training datasets
- Synthetic data generation must follow established privacy and security protocols

20.3 AI Transparency and Accountability

- AI systems must provide explainable outputs where decisions impact individuals, in accordance with GDPR Article 22 requirements for automated decision-making
- Users interacting with AI-generated content or recommendations must be informed that AI is involved
- Human oversight is required for AI systems making decisions that materially affect individuals
- AI system behavior is logged and auditable, with outputs traceable to specific model versions and input data

20.4 Generative AI Controls

The use of generative AI tools (including but not limited to large language models, code generation tools, and image generation systems) is subject to the following controls:

- Company-approved generative AI tools may be used for business purposes in accordance with usage guidelines published by the Information Security team
- Restricted and Confidential data must not be entered into external generative AI services unless the service has been formally assessed and approved by the Security and Legal teams, with a Data Processing Agreement in place
- AI-generated code must undergo the same code review and security testing processes as human-written code
- AI-generated content intended for external distribution must be reviewed for accuracy and appropriateness by a qualified human reviewer

21. Policy Enforcement and Exceptions

21.1 Compliance Monitoring

Meridian Health employs technical and administrative measures to monitor compliance with this Policy:

- Automated compliance scanning tools continuously monitor system configurations against policy requirements
- The GRC team conducts periodic spot checks and policy compliance reviews
- Internal audit includes assessment of policy compliance in its annual audit plan
- Metrics on policy compliance are reported to executive leadership quarterly

21.2 Disciplinary Action

Violations of this Policy or any subsidiary information security policies may result in disciplinary action up to and including termination of employment or contract. The severity of disciplinary action will be proportional to the nature and impact of the violation:

- **Minor violations (first offense, no data exposure):** Written warning and mandatory remedial training
- **Moderate violations (repeated minor violations or single significant violation):** Formal disciplinary action, potential suspension of system access, mandatory counseling
- **Severe violations (intentional misconduct, data breach, regulatory non-compliance):** Termination of employment or contract, potential legal action, and regulatory notification as required

Disciplinary proceedings are managed by Human Resources in consultation with the CISO and General Counsel.

21.3 Policy Exceptions

Exceptions to this Policy may be granted under the following conditions:

- A formal exception request must be submitted in writing to the CISO, documenting the specific policy requirement for which an exception is requested, the business justification, the compensating controls that will be implemented, and the requested duration
- Exceptions must be approved by the CISO for Tier 2 and Tier 3 policy requirements, or by the Board Security Committee for Tier 1 (this Policy) requirements
- All exceptions are time-limited (maximum 12 months) and must be reviewed at expiration

- A risk assessment must be conducted for each exception, and the residual risk must be formally accepted by the appropriate risk owner
- Active exceptions are tracked in the risk register and reported to executive leadership quarterly

Appendix A: Definitions and Glossary

Term	Definition
Availability	The property of information and systems being accessible and usable upon demand by authorized users
CIA Triad	The three fundamental information security objectives: Confidentiality, Integrity, and Availability
Compensating Control	An alternative security control implemented when a primary control cannot be applied, providing equivalent or comparable protection
Confidentiality	The property of information not being disclosed to unauthorized individuals, entities, or processes
Data Controller	The entity that determines the purposes and means of processing personal data (GDPR definition)
Data Processor	The entity that processes personal data on behalf of the controller (GDPR definition)
Data Subject	An identified or identifiable natural person to whom personal data relates (GDPR definition)
EDR	Endpoint Detection and Response — a security solution that monitors endpoint devices for malicious activity
FIPS	Federal Information Processing Standards — US government standards for information processing
ISMS	Information Security Management System — a systematic approach to managing sensitive information
Integrity	The property of accuracy and completeness of information assets
KRI	Key Risk Indicator — a metric used to provide an early signal of increasing risk exposure
MFA	Multi-Factor Authentication — authentication requiring two or more verification factors
MTPD	Maximum Tolerable Period of Disruption — the maximum time a business process can be unavailable
PAM	Privileged Access Management — solutions for managing and securing privileged access to critical assets
PHI	Protected Health Information — individually identifiable health information as defined by HIPAA
PII	Personally Identifiable Information — information that can be used to identify, contact, or locate a specific individual
RPO	Recovery Point Objective — the maximum acceptable amount of data loss measured in time
RTO	Recovery Time Objective — the maximum acceptable time to restore a system after disruption
SIEM	Security Information and Event Management — a system that aggregates and analyzes security events from across the enterprise

Term	Definition
SOC	Security Operations Center — the team and facility responsible for monitoring and responding to security events
Zero Trust	A security model based on the principle of "never trust, always verify" — no implicit trust is granted based on network location or identity

Appendix B: Regulatory Control Cross-Reference

This appendix maps key sections of this Policy to the applicable regulatory and framework control requirements.

Policy Section	SOC 2 TSC	ISO 27001	HIPAA	NIST CSF 2.0	PCI DSS 4.0
2. Governance	CC1.1-CC1.5	5.1, 5.2, 5.3	§164.308(a)(1)	GV.OC, GV.RM	12.1, 12.4
3. Risk Management	CC3.1-CC3.4	6.1, 8.2, 8.3	§164.308(a)(1)(ii)	GV.RM, ID.RA	6.1, 12.2
4. Data Classification	CC6.1, CC6.7	A.5.12-5.14	§164.312(a)	ID.AM	3.1-3.7, 9.4
5. Access Control	CC6.1-CC6.8	A.5.15-5.18, A.8.3-8.5	§164.312(a)(1)	PR.AA	7.1-7.3, 8.1-8.6
6. Network Security	CC6.1, CC6.6	A.8.20-8.23	§164.312(e)(1)	PR.DS, PR.IR	1.1-1.5, 4.1-4.2
7. Endpoint Security	CC6.8	A.8.1, A.8.7	§164.310(d)(1)	PR.DS	5.1-5.4, 9.5
8. Cryptography	CC6.1, CC6.7	A.8.24	§164.312(a)(2)(iv)	PR.DS	3.5, 3.6, 4.1
9. Application Security	CC7.1, CC8.1	A.8.25-8.34	§164.312(a)(1)	PR.DS	6.1-6.5
10. Cloud Security	CC6.1, CC6.7	A.5.23, A.8.26	§164.308(b)(1)	PR.DS, PR.IR	2.2, 6.3
11. Incident Response	CC7.3-CC7.5	A.5.24-5.28	§164.308(a)(6)	RS.MA, RS.AN	10.4, 12.10
12. Physical Security	CC6.4, CC6.5	A.7.1-7.14	§164.310(a)(1)	PR.AC	9.1-9.4
13. Security Awareness	CC1.4	A.6.3	§164.308(a)(5)	PR.AT	12.6
14. Business Continuity	A1.1-A1.3	A.5.29-5.30	§164.308(a)(7)	RC.RP	12.10
15. Vendor Management	CC9.2	A.5.19-5.22	§164.308(b)	GV.SC	12.8, 12.9
17. Monitoring & Logging	CC7.1-CC7.2	A.8.15-8.16	§164.312(b)	DE.CM, DE.AE	10.1-10.7
18. Change Management	CC8.1	A.8.32	§164.308(a)(8)	PR.DS	6.5
20. AI Governance	PI1.1	A.5.36	Emerging guidance	GV.OC	Emerging guidance

Appendix C: Policy Acknowledgment Form

I acknowledge that I have received, read, and understand the Meridian Health Technologies, Inc. Information Security Policy (Document ID: MHT-ISP-2026-001, Version 4.2).

I understand that:

- I am responsible for complying with this Policy and all subsidiary information security policies, standards, and procedures
- Violation of this Policy may result in disciplinary action up to and including termination of employment or contract
- I must report any suspected security incidents, vulnerabilities, or policy violations immediately
- I must complete all required security awareness training within the specified timeframes
- I have no expectation of privacy when using Company information systems

_____	_____
Employee / Contractor Name (Print)	Date
_____	_____
Signature	Employee ID / Contractor ID
_____	_____
Department / Team	Manager Name

Return this signed form to Human Resources within 5 business days of receipt.

Electronic acknowledgment through the Company's policy management system is also accepted.

— End of Document —