



TeleHealthcare
Network

Augmenting Care Through Virtual Coverage

PRIVACY AND DATA PROTECTION POLICY

TELEHEALTHCARE NETWORK

Governing the collection, use, disclosure, retention, and destruction of customer and patient personal data across all TeleHCN products and services

Version 1.0

Effective Date: 1 January 2026

Date Adopted: 4 October 2026

Policy Owner: Vimarsh Raina, MD — Privacy Officer

Approved by: Vimarsh Raina, MD — Chief Executive Officer

Review Cycle: Annually, and upon material regulatory or operational change

1. Purpose

This Privacy and Data Protection Policy ("Policy") establishes how TeleHealthcare Network ("TeleHCN" or the "Company") collects, uses, discloses, transfers, secures, retains, and destroys personal data entrusted to it by its customers, by the patients those customers serve, and by its own personnel, in the course of delivering TeleHCN products and services.

The Policy exists to satisfy four objectives:

1. Ensure that personal data processed by or on behalf of TeleHCN is handled lawfully, and only for the purposes for which it was entrusted to us.
2. Give customers, business partners, and regulators a single authoritative statement of TeleHCN's privacy commitments that can be relied upon in contracting and third-party risk assessment.
3. Give every person who touches customer data an unambiguous set of rules, and a defined consequence for breaking them.
4. Demonstrate an operating privacy program — not merely a written commitment — through assigned accountability, training, monitoring, risk assessment, and enforcement.

This Policy is the governing internal document of the TeleHCN privacy program. It is distinct from the TeleHCN Notice of Privacy Practices, which is a patient-facing HIPAA disclosure, and from the TeleHCN Code of Conduct, which states broader ethical and professional obligations. Where those documents address the same subject, this Policy controls on matters of data handling.

2. Scope and Applicability

2.1 Who This Policy Binds

This Policy applies in full, and without distinction, to:

- All TeleHCN employees, full-time, part-time, and per diem;
- All officers and members of the Board of Directors or governing body;
- All independent contractors and contracted clinicians, including physicians, nurse practitioners, and physician assistants engaged under a TeleHCN agreement;
- All temporary, locum tenens, per-assignment, and agency personnel;
- All suppliers, subcontractors, vendors, consultants, and business partners who process personal data on TeleHCN's behalf or receive personal data from TeleHCN.

Employees and Contractors Are Held to Identical Standards

Every obligation in this Policy — training, access control, US-only work location, incident reporting, monitoring, audit, and sanctions — applies to contracted clinicians and contractors on the same terms as to employees. Contractor status does not reduce any requirement, shorten any timeline, or soften any consequence.

For contractors, these obligations are imposed contractually through the independent contractor agreement, the business associate or subcontractor agreement, and by reference to this Policy. Failure to meet them is a breach of contract and grounds for immediate removal from assignment and termination.

2.2 What Data This Policy Covers

This Policy covers all personal data that TeleHCN processes in any form — electronic, paper, verbal, or visual — at any point in its lifecycle, including:

- **Patient personal data and protected health information (PHI)** accessed, created, received, transmitted, or maintained in connection with clinical services delivered to customer facilities;
- **Customer personal data** relating to customer employees, clinicians, administrators, and other individuals at customer organizations, including contact details, credentials, schedules, and communications;
- **Clinician and workforce personal data**, including credentialing files, licensure records, background check results, and payroll information;
- **Prospect and business contact data** collected through sales, marketing, and website activity.

2.3 What This Policy Does Not Cover

This Policy does not govern data held solely within a customer facility's own systems and never transferred to or accessed by TeleHCN, nor does it displace the terms of an executed Business Associate Agreement ("BAA"), Data Processing Agreement, or master services agreement with a customer. Where a customer agreement imposes a stricter requirement than this Policy, the customer agreement controls for that customer's data, and TeleHCN will meet the stricter standard.

2.4 Legal and Regulatory Framework

TeleHCN operates exclusively within the United States and structures its privacy program around United States federal and state law. The primary instruments are:

- The Health Insurance Portability and Accountability Act of 1996, the HITECH Act, and the implementing Privacy, Security, and Breach Notification Rules at 45 C.F.R. Parts 160 and 164;
- 42 C.F.R. Part 2, governing records of substance use disorder treatment;
- State health privacy, medical records, and telehealth statutes in each state where TeleHCN operates or where a patient is located at the time of service;
- State consumer privacy statutes, including the California Consumer Privacy Act as amended, and comparable laws in other states, to the extent they apply to data outside the HIPAA exemption;
- State data breach notification statutes in all applicable jurisdictions;
- The Federal Trade Commission Act, Section 5, as it applies to representations made about privacy and security practices.

TeleHCN does not offer services to individuals located outside the United States and does not knowingly process personal data subject to the EU or UK General Data Protection Regulation. If TeleHCN's operations change such that a non-US regime applies, this Policy will be amended before that processing begins, under the process in Section 17.

3. Governance: Roles and Responsibilities

Accountability for privacy at TeleHCN is assigned to named individuals, not to the organization generally. Every person listed below has defined responsibilities, and every person with access to customer data has a defined role.

Role	Primary Responsibilities	Accountable For
Chief Executive Officer	Approves this Policy and material amendments; allocates resources to the privacy program; receives escalation of Critical incidents and unremediated High risks.	Ultimate accountability for the privacy program and for the adequacy of resourcing.
Privacy Officer	Owns this Policy. Administers individual rights requests, privacy complaints, annual privacy risk assessments, DPIAs, and the retention schedule. Approves the categories of data that may be processed. Maintains the record of processing activities.	Program design, regulatory interpretation, rights request fulfilment within legal deadlines, and annual policy review.
Security Officer	Owns technical and physical safeguards: access provisioning and review, encryption standards, endpoint and network controls, logging and alerting, vulnerability management, and technical incident containment.	Effectiveness of security controls and the technical response to security incidents.
Compliance Officer	Monitors and audits compliance with this Policy; administers the sanctions process; tracks training completion; maintains the exceptions register.	Detection of non-compliance and consistent application of sanctions.
Clinical Leadership	Ensures clinicians access records only for legitimate treatment purposes; reviews clinical escalations arising from privacy incidents.	Clinician conduct at the point of care.
Human Resources and Credentialing	Executes onboarding and offboarding checklists; verifies training completion before access is granted; verifies US work location attestations; revokes access on separation.	That no person receives access before completing prerequisites, and that access ends on separation.
Contract and Vendor Owners	Conduct third-party privacy due diligence; ensure BAAs, subcontractor agreements, and data protection terms are executed before data is shared; conduct annual vendor review.	That no personal data reaches a third party without an executed agreement.
All Workforce Members and Contracted Clinicians	Comply with this Policy; complete assigned training; access only the minimum data necessary; report suspected incidents within 24 hours.	Their own conduct and the security of credentials and devices issued to them.

3.1 Segregation and Least Privilege

Access to customer personal data is granted by role, not by seniority. Each role has a documented data access profile specifying the systems, record types, and fields that role may reach. No person receives access outside their profile without written approval from the Privacy Officer and the Security Officer, and every such exception is recorded in the exceptions register with an expiry date.

3.2 Named Officers and Contact Details

The following individuals hold the designated privacy and security roles for TeleHealthcare Network. Questions about this Policy, requests to exercise a privacy right, reports of a suspected incident, and requests for evidence in support of third-party risk assessment should be directed to them.

Role	Name	Email	Telephone
Privacy Officer	Vimarsh Raina, MD	dr.raina@telehealthcarenetwork.com	715-321-4122
Security Officer	Cesar Ramirez	cesar@telehealthcarenetwork.com	703-914-3000
Compliance Officer	Vimarsh Raina, MD	dr.raina@telehealthcarenetwork.com	715-321-4122

Where one individual holds more than one of these roles, the CEO documents the assignment and identifies an independent reviewer for matters where the roles would otherwise conflict.

4. Collection, Use, Disclosure, and Retention in Our Products and Services

This Section states how personal data moves through TeleHCN's services. It is the operative answer to what TeleHCN does with customer data.

4.1 Collection

TeleHCN collects personal data only from these sources and only for the purposes stated:

Source	Data Collected	Purpose of Collection
Customer facility clinical systems (EHR, PACS, lab)	Patient demographics, clinical history, orders, results, notes, imaging.	To deliver remote clinical care under the customer's direction. Accessed in place wherever technically possible; not copied to TeleHCN systems.
Telehealth encounter platform	Encounter metadata: date, time, duration, participating clinician, facility, patient identifier.	To evidence that contracted coverage was delivered, to support billing, and to enable quality review.
Customer administrative contacts	Name, title, work email, work phone, facility, scheduling preferences.	To administer the service relationship, coordinate coverage, and provide support.

Source	Data Collected	Purpose of Collection
Clinicians and applicants	Licensure, DEA registration, credentialing and privileging records, background checks, malpractice history, tax and payment details.	To credential, engage, schedule, and pay clinicians, and to meet customer credentialing obligations.
Website and marketing channels	Business contact details voluntarily submitted; limited analytics data.	To respond to enquiries and administer business development. No patient data is collected through these channels.

TeleHCN does not purchase personal data from data brokers, does not collect personal data through undisclosed means, and does not use customer or patient personal data to train artificial intelligence or machine learning models.

4.2 Use

Personal data is used only for the purpose for which it was collected, and for compatible purposes that the customer would reasonably expect. Permitted uses are:

- Delivering, coordinating, and documenting clinical care;
- Billing, invoicing, and substantiating contracted coverage;
- Quality assurance, peer review, credentialing, and clinical supervision;
- Responding to customer support requests and service issues;
- Meeting legal, regulatory, accreditation, and contractual obligations;
- Security monitoring, audit, and incident investigation;
- Publishing a clinician's professional profile and photograph on Company channels and in proposals, where that clinician has given written permission and may withdraw it at any time (see Section 5.2).

Any use outside this list requires prior written approval from the Privacy Officer, and where the data belongs to a customer, prior written approval from that customer.

4.3 Disclosure

TeleHCN discloses personal data only:

- Back to the customer facility that owns the record, and to other providers involved in the patient's care;
- To subcontractors and suppliers bound by an executed BAA or equivalent data protection agreement, and only to the extent necessary for them to perform;
- Where required by law, or in response to valid legal process, after review by the Privacy Officer;
- With the written authorization of the individual or the customer.

TeleHCN does not sell personal data, does not share personal data for cross-context behavioural advertising, and does not disclose personal data for any commercial purpose unrelated to the services. These commitments are absolute and are not subject to exception.

4.4 Retention

Personal data is retained only as long as necessary for the purpose for which it was collected, or as required by law or customer contract, whichever is longer. The governing schedule is at Section 11. At the end of the retention period the data is destroyed using the methods in Section 11.3.

4.5 Data Ownership

Patient records created in a customer facility's systems remain the property and legal record of that customer. TeleHCN acts on the customer's behalf and asserts no ownership over customer or patient personal data. On termination of a customer relationship, TeleHCN returns or destroys customer personal data as directed by the customer under Section 9.4.

4.6 Record of Processing Activities

TeleHCN maintains a Record of Processing Activities (the "Record") — a single, current inventory of every activity through which it processes personal data. The Record is a standing artefact of the privacy program, not a document produced on demand in response to a customer enquiry.

Contents. For each processing activity the Record states: the activity and its reference; whether TeleHCN acts as a business associate or as data owner in its own right; the categories of data subject; the categories of personal data; the purpose; the legal or contractual permission; the source of the data; the categories of recipient; the systems involved; the storage and access location; the retention period; and the safeguards specific to that activity. The Record also contains documented data flow diagrams, a system and storage inventory, and a register of recipient categories.

Ownership and maintenance. The Privacy Officer owns the Record and is accountable for its accuracy and completeness. It is reviewed in full at least annually, timed to run alongside the annual privacy risk assessment at Section 12 so that the Record is validated as the assessment is scoped, and the review is logged in its version history whether or not any entry changes. At each Quarterly Privacy and Security Management Review under Section 13.3, system and contract owners confirm in minuted form that no processing activity has been added, altered, or retired without a corresponding update.

Triggered updates. The Record is updated within 30 days of any event that triggers a privacy risk assessment under Section 12.2 — a new product, service, data category, purpose, supplier, system, hosting change, customer segment, or state of operation, and the retirement of any of these — together with any change in a supplier's processing or support location, any change to the retention schedule, and any finding from an assessment, audit, incident, or customer enquiry. Any workforce member may raise a trigger. The trigger list is deliberately identical to that at Section 12.2 so that the Record and the risk assessment never fall out of step.

Validation. Annual review is not self-certified. The Privacy Officer validates the Record against independent sources — the supplier register and executed agreements, the identity provider's inventory of provisioned systems and users, hosting region configuration exports, and a sample of access logs. Any system in use but absent from the Record, or recorded but no longer in use, is a finding entered in the privacy risk register with a mitigation plan under Section 13.

Availability. The Record, including its data flow diagrams, is available to customers and prospects conducting third-party risk assessment, under NDA where appropriate. Systems and suppliers are identified in the external Record by function rather than by vendor name; a separate internal System and Supplier Register naming each one is available under NDA on request.

5. Data Minimization, Purpose Limitation, and Confidentiality

All processing of personal data by TeleHCN is subject to the following binding principles. They are not aspirational statements; they are the standard against which the Compliance Officer audits under Section 19.

5.1 Data Minimization

TeleHCN collects, accesses, and retains the least personal data required to accomplish the purpose, and no more. In practice this means:

- Clinicians access only the records of patients for whom they are providing care during the shift in question, and only the portions of those records relevant to the clinical question.
- Systems are configured to expose the minimum necessary fields by role. Where a system cannot enforce field-level restriction, compensating audit controls apply.
- Data is accessed in the customer's system in place wherever technically possible, rather than copied to TeleHCN systems. Local copies, downloads, exports, screenshots, and printing of patient data are prohibited absent documented approval.
- Reports, analytics, and quality reviews use de-identified or aggregated data unless identifiers are strictly necessary to the analysis.
- Requests to suppliers and subcontractors are scoped to the minimum data set they need to perform, and are documented in the applicable agreement.

The HIPAA minimum necessary standard applies to all uses, disclosures, and requests other than those the rule excludes — disclosures to or requests by a provider for treatment, disclosures to the individual, disclosures under a valid authorization, and disclosures required by law.

5.2 Purpose Limitation

Personal data is processed only for the specific purposes stated in Section 4.2 and, where applicable, in the executed customer agreement. TeleHCN does not repurpose customer personal data. Specifically, TeleHCN does not:

- Use one customer's data to benefit, benchmark, or market to another customer;
- Use patient or customer data for product development, model training, or research without a separate written agreement and, where required, IRB approval and authorization;
- Use clinician credentialing data for any purpose other than credentialing, engagement, scheduling, payment, and customer verification. The one exception is a clinician's professional profile — name, credentials, specialty, education, years of experience, states of licensure, languages and a short biography, with a photograph — which may be published on Company channels and used in proposals where that clinician has given written permission in their engagement agreement. Profile Materials are held separately from the credentialing file, are never accompanied by licence, DEA or NPI numbers, background check results or compensation, and are removed within 30 days of withdrawal or the end of the engagement (Record of Processing Activities, PA-11);
- Retain data after its purpose has been served on the basis that it may prove useful later.

A proposed new purpose requires a documented purpose-change assessment by the Privacy Officer, evaluating compatibility with the original purpose, the applicable customer agreement, and legal basis, before any processing begins.

5.3 Confidentiality

Every person covered by this Policy is bound to confidentiality as a condition of engagement:

- Confidentiality obligations are imposed in writing before access is granted, through the employment agreement, independent contractor agreement, or a standalone confidentiality agreement, and are reinforced by the Code of Conduct acknowledgment.
- Personal data is discussed only with those who have a legitimate need to know, and never in public or semi-public settings — including shared workspaces, corridors, vehicles, and open household areas during remote shifts.
- Accessing a record out of curiosity, or accessing the record of a coworker, family member, neighbour, public figure, or oneself outside a treatment relationship, is prohibited and is grounds for immediate termination.
- Confidentiality obligations survive the end of employment or contract indefinitely.

5.4 Additional Principles

- **Accuracy.** Personal data is kept accurate and current. Errors identified in clinical documentation are corrected through a properly attributed addendum, never by silent alteration.
- **Integrity and availability.** Controls protect data against unauthorized alteration and against loss, including tested backup and recovery.
- **Transparency.** TeleHCN accurately describes its data practices to customers and does not make privacy or security representations it cannot substantiate.
- **Accountability.** TeleHCN maintains records sufficient to demonstrate compliance with this Policy, including training records, access logs, risk assessments, and incident files.

5.5 Data Accuracy: Verification and Audit

TeleHCN maintains a defined process to verify that personal data it holds or records is accurate, complete, and current. Because accuracy matters differently by data type, the controls differ by data type. The operating detail is set out at Section 9 of the Record of Processing Activities.

Clinical documentation

- Clinicians document contemporaneously and record only what they actually did. Cloned documentation and templated text that does not reflect the encounter are prohibited.
- Errors are corrected by a properly attributed, dated addendum that preserves the original entry. Silent alteration or backdating of a record is prohibited and is grounds for termination.
- Correction is made in the customer facility's system under that facility's amendment process. TeleHCN does not maintain a parallel copy that could diverge from the legal record.
- Peer review and quality assurance sample documentation for accuracy and completeness, and findings are recorded in the clinician's credentialing file.

Credentialing and workforce data

- Licensure, DEA registration, and board certification are verified at primary source with the issuing authority at engagement, and re-verified ahead of each expiry date rather than on a fixed calendar.
- Exclusion and sanctions screening against the OIG LEIE, GSA SAM, OFAC SDN, and applicable state exclusion lists including the New York State Medicaid Exclusion List is re-run monthly, so that a change in status is detected within 30 days.

- Clinicians must notify the Compliance Officer within three business days of any change to licence status, disciplinary action, malpractice claim, privileging decision, criminal charge, or insurance coverage.
- Each individual confirms in writing the accuracy of their credentialing record, contact details, licensure states, and attested US work location at each annual training cycle.

Coverage, billing, and business data

- Encounter metadata is generated automatically by the telehealth platform rather than keyed by hand, removing the most common source of transcription error.
- Invoices are reconciled against platform-generated encounter records before issue, and customers are invited to confirm coverage records against their own logs at each billing cycle.
- Business contact data is corrected on notification or delivery failure, reviewed at contract renewal, and purged at its retention limit, since stale contact data is inaccurate data.

Individual-initiated correction and audit

Any individual may request correction under Section 10.1; requests concerning patient clinical records are routed to the customer facility within five business days under Section 10.2. Scheduled accuracy audits — credentialing file sampling, monthly exclusion screening, annual self-attestation, billing-cycle reconciliation, ongoing documentation review, and annual validation of the Record of Processing Activities — are performed on the cadence set at Section 9 of that Record. Accuracy failures are entered in the privacy risk register and, where systemic rather than isolated, carry a documented mitigation plan with a named owner under Section 13.

6. Restrictions on the Types of Personal Data Processed

TeleHCN restricts, by policy and by system configuration, the categories of customer personal data that may be processed through its products and services. Data outside the permitted set must not be transmitted to, entered into, or stored in any TeleHCN system.

Category	Status	Conditions and Controls
Patient demographics and identifiers required for treatment	Permitted	Accessed in the customer system in place. Minimum necessary applies.
Clinical data required for the encounter	Permitted	Accessed for the shift and clinical question at hand only.
Encounter metadata	Permitted	Retained in TeleHCN systems to evidence coverage and support billing.
Customer business contact data	Permitted	Work contact details only. No personal home addresses or personal contact details.
Clinician credentialing and payment data	Permitted	Restricted to Credentialing and Finance roles. Encrypted at rest with field-level access control.

Category	Status	Conditions and Controls
Substance use disorder treatment records (42 C.F.R. Part 2)	Restricted	Processed only where the customer agreement expressly provides, with Part 2 consent requirements and re-disclosure notices applied.
Payment card data	Prohibited	TeleHCN does not accept or store cardholder data. Payments are handled by a PCI-DSS compliant processor; card data never enters TeleHCN systems.
Biometric identifiers and genetic data	Prohibited	Not collected or processed. Prohibited absent a written exception approved by the Privacy Officer and the CEO.
Patient financial account and Social Security numbers	Prohibited	Not required for clinical services. Must not be transmitted to TeleHCN; if received in error, handled under Section 6.2.
Consumer or third-party data acquired from brokers	Prohibited	TeleHCN does not purchase or ingest broker data.
Data of individuals located outside the United States	Prohibited	Outside the scope of TeleHCN services. See Section 9.

6.1 Enforcement of the Restriction

The restriction is enforced through three layers: contractual terms limiting the data customers may transmit to TeleHCN; system configuration and data loss prevention controls that block prohibited categories where technically feasible; and periodic sampling by the Compliance Officer under Section 19.

6.2 Unsolicited or Erroneous Receipt

If prohibited data is received in error, the recipient must not open, copy, or forward it, and must notify the Privacy Officer within 24 hours. The Privacy Officer will arrange secure deletion, notify the sender, record the event in the incident register, and determine whether it constitutes a reportable incident under Section 11.

6.3 Adding a New Data Category

Introducing a new category of personal data into any TeleHCN product or service requires a privacy risk assessment under Section 12 and written approval from the Privacy Officer before processing begins. New categories are added to the table above by amendment under Section 17.

7. Data Residency, Cross-Border Access, and Transfers

United States Only — No Exceptions

All personal data processed by or on behalf of TeleHealthcare Network is stored, processed, and accessed exclusively within the United States.

No employee, contracted clinician, contractor, supplier, subcontractor, or support resource may access customer or patient personal data from any location outside the United States, at any time, for any reason. This prohibition applies to production access, support access, administrative access, and read-only access alike.

TeleHCN does not offshore, nearshore, or subcontract any function that touches customer personal data.

7.1 Storage Location

All TeleHCN systems that store personal data, and all backups and disaster recovery copies, are hosted in data centres located within the United States. Cloud services are contractually configured to US-only regions, and configuration is verified at onboarding and at each annual vendor review. Replication of data outside the United States is contractually prohibited and disabled in configuration.

7.2 Personnel Location

Every person granted access to customer personal data must be physically located within the United States or its territories at the time of access. This is enforced as follows:

- Every employee and contracted clinician attests in writing, at onboarding and at each annual training cycle, that they will access TeleHCN and customer systems only from within the United States.
- The requirement is a term of the employment agreement and of every independent contractor agreement, and its breach is a material breach of contract.
- Access from a non-US IP address is blocked at the network and identity provider layer where technically supported, and generates an alert to the Security Officer where a block cannot be applied.
- Use of a VPN, proxy, remote desktop, or other means to disguise access location, or to access TeleHCN or customer systems from outside the United States, is treated as intentional circumvention and results in immediate termination.
- The prohibition applies at all times, including while travelling. No person may access customer or patient personal data from outside the United States for any reason, and access while abroad is not permitted even temporarily or with approval.

7.3 Suppliers and Subcontractors

Before any supplier or subcontractor receives or accesses personal data, the Contract Owner must confirm and document that:

1. The supplier stores and processes the data exclusively in the United States;
2. All supplier personnel with access to the data — including support, engineering, and administrative staff — are located within the United States;
3. The supplier is contractually prohibited from transferring the data outside the United States or granting access from outside the United States, including to its own affiliates and subcontractors;
4. The supplier is contractually required to notify TeleHCN before engaging any onward subcontractor, and to flow down these same restrictions.

A supplier that cannot meet these conditions is not approved, irrespective of commercial considerations. Existing suppliers are re-verified at each annual vendor review, and any change in a supplier's processing or support location must be notified to TeleHCN in advance and triggers reassessment.

7.4 Onward Transfer Prohibition

TeleHCN does not transfer customer or patient personal data to any recipient outside the United States in the delivery of its services. No such data is transferred to a foreign government, foreign affiliate, or foreign processor, and no supplier stores, processes, supports or accesses it from outside the United States. If TeleHCN receives a request for personal data from a non-US authority, it will not respond substantively and will refer the request to the Privacy Officer and to legal counsel immediately.

7.5 The One Exception: TeleHCN's Own Advisers and Insurers

Section 7.4 governs the storage, processing, support and routine access of personal data in the delivery of TeleHCN's services. It does not prevent TeleHCN from meeting a legal or contractual obligation to its own insurer, regulator or legal adviser, one of which — its cyber liability insurer, CFC Underwriting Limited — is established in the United Kingdom. Where such an obligation requires disclosure of personal data outside the United States:

- The disclosure is limited to what the obligation actually requires, and the initial notification of an incident contains no protected health information and no personal identifiers;
- Any disclosure of identifiable information is approved in writing by the Privacy Officer, recorded in the matter file, and limited to the minimum necessary;
- The disclosure is recorded as an onward transfer in the Record of Processing Activities and reported to the affected customer where it concerns their data;
- The arrangement is reviewed annually, including whether a United States-established alternative is available on comparable terms.

The operating detail is at Section 10.4 of the Incident Response Plan. No other exception to Section 7 exists, and Section 19.6 continues to prohibit any exception being granted.

7.6 Verification and Evidence

The Security Officer produces, at least annually and on customer request, evidence of data residency comprising: the current system and hosting inventory with region configuration; the supplier register with attested processing and support locations; access log analysis showing source geography; and the roster of personnel with data access and their attested work locations. This evidence is retained under Section 9 and is available to customers under NDA as part of third-party risk assessment.

8. Personal Data Security Measures

TeleHCN maintains administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of personal data, in accordance with the HIPAA Security Rule at 45 C.F.R. Part 164 Subpart C. Safeguards are reviewed at least annually and after any material change in systems or threat environment.

8.1 Administrative Safeguards

- A designated Security Officer with assigned authority and accountability;
- Documented risk analysis and risk management processes, executed at least annually under Section 12;

- Role-based access authorization, with access granted only after training completion and only to the documented role profile;
- Workforce clearance procedures, including identity verification, licensure primary source verification, background checks, and exclusion screening;
- Quarterly user access reviews, with attestation by the system owner and removal of access no longer required;
- Documented sanctions for policy violation, applied under Section 19;
- Written agreements with every supplier and subcontractor before data is shared, under Section 14;
- Contingency planning, including data backup, disaster recovery, and emergency mode operation, with restoration tested at least annually.

8.2 Technical Safeguards

- **Encryption in transit.** TLS 1.2 or higher for all transmission of personal data across any network. Unencrypted transmission of personal data is prohibited.
- **Encryption at rest.** AES-256 or equivalent for personal data at rest, including databases, file storage, backups, and full-disk encryption on every endpoint used to access personal data.
- **Unique identification.** Every user has an individual account. Shared, generic, and service accounts with interactive access are prohibited, so that every access is attributable to one person.
- **Multi-factor authentication.** Required for all access to systems containing personal data, all remote access, and all administrative access, without exception.
- **Least privilege and just-in-time elevation.** Standing administrative privilege is minimized; elevation is time-bound, justified, and logged.
- **Automatic logoff.** Sessions terminate after a defined period of inactivity; devices lock automatically.
- **Audit controls.** Access to personal data is logged at the record level where the system supports it. Logs are protected against alteration, retained for six years, and reviewed under Section 19.
- **Endpoint protection.** Managed endpoint detection and response, enforced patching, host firewall, and device encryption on every device permitted to access personal data. Unmanaged personal devices are not permitted to access personal data.
- **Network controls.** Segmentation, firewalling, intrusion detection, and geographic access restriction under Section 7.2.
- **Vulnerability management.** Regular vulnerability scanning, with remediation timelines by severity, and annual penetration testing of internet-facing systems.
- **Data loss prevention.** Controls to detect and block unauthorized export, download, printing, or transmission of personal data, including to personal email and consumer file-sharing services.

8.3 Physical Safeguards

- Facility access controls at TeleHCN premises, and reliance on the physical security programs of certified US data centre providers for hosted systems;
- Workstation use policy requiring clinicians to work from private, secure locations where screens and conversations cannot be observed, with privacy filters in shared environments;
- Device and media controls governing issuance, tracking, reuse, and disposal, including sanitization before reuse and certified destruction at end of life;

- Prohibition on removable media for personal data absent written approval and encryption.

8.4 Prohibited Practices

The following are prohibited for all personnel, employees and contractors alike, and are enforced as serious violations:

- Transmitting personal data by personal email, personal SMS, or consumer messaging applications;
- Entering personal data into any artificial intelligence tool, transcription service, translation service, or cloud service not approved in writing by the Security Officer and covered by an executed agreement;
- Storing personal data on personal devices, personal cloud accounts, or removable media;
- Sharing credentials, or permitting another person to use an account issued to you;
- Photographing or screen-recording any system displaying personal data;
- Disabling, bypassing, or attempting to circumvent any security control.

8.5 Secure Development and Change Management

Changes to systems that process personal data follow a documented change management process including security review, testing in an environment containing no live personal data, approval, and rollback planning. Production personal data is never used in development, test, or training environments; where realistic data is required it is synthetic or de-identified in accordance with 45 C.F.R. § 164.514.

9. Data Retention and Destruction

TeleHCN retains personal data only for as long as it is needed for the purpose for which it was collected, or for the period required by law, regulation, or customer contract, whichever is longer. Indefinite retention "in case it is useful" is prohibited.

9.1 Retention Schedule

The Privacy Officer maintains the retention schedule below and reviews it annually. Where a customer agreement specifies a different period, the customer agreement controls for that customer's data.

Record Type	Retention Period	Basis and Notes
Patient clinical records held in customer systems	Not retained by TeleHCN	Legal record of the customer facility. TeleHCN accesses in place and retains no copy.
Encounter metadata and shift/coverage logs	7 years from encounter	Evidence of contracted coverage; supports billing substantiation and malpractice defence.
Billing, invoicing, and payment records	7 years from creation	Tax, audit, and False Claims Act limitations considerations.
Clinician credentialing and privileging files	Engagement + 6 years	Customer credentialing obligations and HIPAA §164.316(b)(2) documentation retention.
System and record access audit logs	6 years from creation	45 C.F.R. §164.316(b)(2)(i).

Record Type	Retention Period	Basis and Notes
Security and privacy incident files	6 years from closure	HIPAA documentation retention; breach notification evidence.
Privacy risk assessments and mitigation plans	6 years from completion	Evidence of an operating privacy program.
Training records and completion attestations	6 years from completion	45 C.F.R. §164.530(j).
Business associate and subcontractor agreements	Termination + 6 years	HIPAA documentation retention; surviving obligations.
Individual rights requests and responses	6 years from response	Evidence of timely fulfillment.
Business email and correspondence	3 years, unless subject to legal hold	Operational need; superseded by legal hold.
Applicant records for unsuccessful candidates	1 year from decision	EEOC recordkeeping.
System backups	35 days rolling	Overwritten on cycle. Deletion requests are applied to production immediately and propagate through backup expiry.

9.2 Legal Hold

When litigation, an investigation, an audit, or a regulatory inquiry is reasonably anticipated, the Privacy Officer issues a written legal hold suspending destruction of the affected records. Scheduled destruction does not resume until the hold is lifted in writing. Destroying, altering, or concealing data subject to a hold is a serious violation and may be a crime.

9.3 Destruction Methods

At the end of the retention period, or on customer instruction, data is destroyed so that it cannot be reconstructed, using methods consistent with NIST SP 800-88:

- **Electronic records:** cryptographic erasure or secure overwrite; deletion from production, replicas, and search indexes, with backup copies expiring on the normal cycle.
- **Storage media and devices:** sanitization before reuse; physical destruction (shredding, disintegration, or degaussing) at end of life by a vetted vendor providing a certificate of destruction.
- **Paper records:** cross-cut shredding or destruction by a bonded vendor providing a certificate of destruction. Paper containing personal data is never placed in ordinary waste or recycling.

The Security Officer records each destruction event — what was destroyed, when, by what method, and by whom — and retains certificates of destruction for six years.

9.4 Return or Destruction at Contract End

On termination of a customer agreement, TeleHCN returns or destroys all customer personal data in its possession as the customer directs, within 30 days of the effective date of termination unless the agreement

specifies otherwise, and certifies completion in writing. Where return or destruction is infeasible for a defined subset — for example, data embedded in immutable audit logs or in backups pending expiry — TeleHCN identifies that subset to the customer, extends the protections of this Policy and the BAA to it for as long as it is retained, and limits further use to the purpose that makes destruction infeasible.

10. Individual Rights Management

TeleHCN maintains a documented process for receiving, verifying, tracking, and fulfilling requests from individuals to exercise their privacy rights, and for assisting customers in meeting their own obligations to individuals.

10.1 Rights Recognized

Right	What TeleHCN Does	Standard Timeline
Access / copy	Provides the individual, or the customer on the individual's behalf, with a copy of the personal data held, in the form and format requested where readily producible, including electronic copy.	30 days; one 30-day extension with written notice of the reason.
Correction / amendment	Corrects inaccurate or incomplete data. Clinical records are corrected by attributed addendum, never silent alteration. Where a request is denied, the reason is given in writing and a statement of disagreement is appended.	60 days; one 30-day extension with written notice.
Deletion / erasure	Deletes data where no legal, contractual, or clinical retention obligation applies, and instructs subcontractors to do the same. Where deletion is not permitted, explains the specific basis for retention.	45 days; one 45-day extension with written notice.
Portability	Provides the data in a structured, commonly used, machine-readable format where the data was provided by the individual or is held electronically in a designated record set.	30 days.
Restriction of processing	Applies and honours agreed restrictions. Honours without exception the HIPAA mandatory restriction where an individual pays in full out of pocket and asks that the item not be disclosed to their health plan.	30 days to respond; restriction applied on acceptance.
Objection to processing	Ceases the objected-to processing where no overriding legal obligation or legitimate basis applies.	30 days.

Right	What TeleHCN Does	Standard Timeline
Confidential communications	Accommodates reasonable requests to receive communications by alternative means or at an alternative location, without requiring an explanation.	Applied on receipt.
Accounting of disclosures	Provides a list of disclosures in the six years preceding the request, excluding those the rule excludes.	60 days; one 30-day extension.
Notification of breach	Notifies affected individuals, or supports the customer in notifying, under Section 11.	Without unreasonable delay; no later than 60 days from discovery.

10.2 Where TeleHCN Acts for a Customer

For patient data held in a customer facility's systems, the customer is the covered entity and owns the relationship with the individual. TeleHCN acts as a business associate. Any rights request TeleHCN receives directly from a patient is acknowledged and forwarded to the customer's privacy contact within five business days, and TeleHCN then provides whatever assistance the customer requires to fulfil the request within the customer's deadline. TeleHCN does not respond substantively to a patient rights request on a customer's behalf without the customer's written direction.

10.3 Intake and Verification

- Requests may be submitted in writing to the Privacy Officer at the contact details in Section 3.2, or through the request form published at telehealthcarenetwork.com.
- The Privacy Officer logs every request in the rights request register on receipt, recording date, requester, right invoked, applicable deadline, and owner.
- Identity is verified proportionately to the sensitivity of the data before any data is disclosed. Where the requester is a personal representative, authority is verified before the request is actioned.
- An acknowledgment is sent within five business days confirming receipt and the applicable deadline.
- No fee is charged for the first request in any 12-month period. Where a fee is permitted for additional or excessive requests, the requester is told the amount in advance and may withdraw or narrow the request.

10.4 Refusal and Appeal

Where a request is refused in whole or in part, the response states the specific reason, the legal basis, and how the individual may appeal internally to the Privacy Officer and complain to the customer facility, to the state authority, and to the HHS Office for Civil Rights. Refusals of access that are subject to review under HIPAA are referred to a licensed health care professional who was not involved in the original decision.

10.5 No Retaliation

No individual is penalized, denied care, or treated differently for exercising a privacy right or making a complaint.

10.6 Metrics

The Privacy Officer reports quarterly to the CEO on rights request volume, type, fulfillment time, and any request that missed its deadline, with the cause and corrective action.

11. Security and Privacy Incident Response

TeleHCN maintains a documented Incident Response Plan, of which this Section states the governing requirements. The plan is tested at least annually through a tabletop exercise, and the results are recorded and used to update the plan.

11.1 Duty to Report — 24 Hours

Every employee and contracted clinician must report any actual or suspected security or privacy incident to the Security Officer and the Privacy Officer immediately, and in no event later than 24 hours after becoming aware of it. Reportable events include lost or stolen devices, misdirected email or messages, suspected phishing or credential compromise, unauthorized access, malware, unavailability of systems, and any impermissible use or disclosure of personal data. Late reporting compresses the time available to meet statutory notification deadlines and is treated as a separate violation of this Policy.

Reports may be made to the Security Officer, the Privacy Officer, or any member of executive leadership. Reporting in good faith is protected; no person is retaliated against for reporting an incident, including one they caused.

11.2 Response Phases

1. Detect and report. Incident identified through monitoring, alerting, user report, customer report, or third-party notification, and logged in the incident register with a unique identifier.
2. Triage and classify. The Security Officer, with the Privacy Officer, assesses scope, data types involved, number of individuals, and whether personal data was accessed or acquired, and assigns a severity under Section 11.3 within 24 hours of report.
3. Contain. Immediate action to stop ongoing exposure — revoking credentials, isolating systems or endpoints, disabling accounts, blocking addresses, remotely wiping devices.
4. Investigate. Determine root cause, full scope, and the data and individuals affected. Preserve evidence and logs; a legal hold is issued where litigation or regulatory action is foreseeable.
5. Notify. Internal, customer, individual, and regulatory notification under Section 11.4.
6. Eradicate and recover. Remove the cause, restore service from verified clean backups, and confirm the vulnerability is closed.
7. Post-incident review. Within 15 business days of closure, a written post-incident report is produced covering timeline, root cause, effectiveness of the response, and corrective actions with named owners and due dates. Corrective actions are tracked to completion under Section 13.

11.3 Severity Classification

Severity	Definition	Response
Critical	Confirmed unauthorized acquisition of personal data; ransomware or systemic compromise; any event likely to require breach notification to 500 or more individuals.	Immediate escalation to CEO and legal counsel. Response team convened within 1 hour. Customer notified within the BAA deadline. Continuous updates until closed.
High	Confirmed impermissible use or disclosure affecting a limited number of individuals; credential compromise with data access; lost or stolen unencrypted device.	Escalation to CEO within 4 hours. Containment same day. Breach risk assessment under Section 11.5 completed within 5 business days.
Medium	Suspected but unconfirmed exposure; misdirected communication contained promptly; policy violation without evidence of data acquisition.	Investigated within 3 business days. Documented risk assessment. Corrective action assigned.
Low	Near miss; blocked attempt; encrypted device lost with no evidence of access.	Logged and reviewed for trend. Corrective action where a pattern emerges.

11.4 Notification Obligations

- **Customer notification.** Where TeleHCN acts as a business associate, the affected customer is notified within the timeframe specified in the executed BAA, and in the absence of a specified timeframe, without unreasonable delay and no later than 5 calendar days from discovery. Notification states what is known, what is not yet known, what has been contained, and when the next update will follow.
- **Individual notification.** Where TeleHCN is the covered entity, affected individuals are notified without unreasonable delay and no later than 60 calendar days from discovery, in plain language, describing what happened, the data involved, steps individuals should take, what TeleHCN is doing, and how to get more information.
- **Regulatory notification.** HHS Office for Civil Rights is notified in accordance with 45 C.F.R. § 164.408 — contemporaneously for breaches affecting 500 or more individuals, and annually for smaller breaches. Media notification is made where a breach affects more than 500 residents of a state or jurisdiction.
- **State notification.** State attorneys general and other state authorities are notified as required by the breach notification law of each affected individual's state of residence, within the deadlines those laws impose.
- **Law enforcement.** Referred where criminal conduct is suspected. A documented law enforcement request may delay notification only to the extent and for the period the law permits.

11.5 Breach Risk Assessment

Any impermissible use or disclosure of protected health information is presumed to be a breach requiring notification unless TeleHCN demonstrates, through a documented risk assessment, that there is a low probability the information has been compromised. The assessment addresses the four factors at 45 C.F.R. § 164.402: the nature and extent of the information involved, including the types of identifiers and the likelihood of re-identification; the unauthorized person who used the information or to whom the disclosure was made; whether the information was actually acquired or viewed; and the extent to which the risk has been mitigated. The assessment is written, signed by the Privacy Officer, and retained for six years.

11.6 Contractor Incidents

Contracted clinicians and contractors are subject to the same 24-hour reporting duty. Supplier and subcontractor agreements require notification to TeleHCN without unreasonable delay and no later than 48 hours from discovery, cooperation in investigation, and provision of all information TeleHCN needs to meet its own notification deadlines.

12. Privacy Risk Assessments

TeleHCN conducts privacy risk assessments of its products and services that touch customer personal data at least annually. The annual assessment is a scheduled, resourced activity owned by the Privacy Officer, not an ad hoc exercise.

12.1 Scope of the Annual Assessment

The annual assessment covers every product, service, system, and process that collects, accesses, transmits, stores, or destroys customer personal data, including services delivered through suppliers and subcontractors. It examines:

- The current inventory of data assets and processing activities, and the categories of data in each — validated against the restrictions in Section 6;
- Data flows into, through, and out of TeleHCN, including every third-party recipient and the residency of each — validated against Section 7;
- The adequacy and operating effectiveness of the safeguards in Section 8;
- Compliance with the minimization, purpose limitation, and confidentiality principles in Section 5;
- Adherence to the retention schedule in Section 9, including evidence that destruction is occurring on schedule;
- The rights request process and its performance against deadlines;
- Incident history since the last assessment, and whether prior corrective actions were completed and effective;
- Changes in applicable law identified under Section 17, and the gap they create.

12.2 Triggered Assessments

In addition to the annual cycle, a privacy risk assessment — or a targeted Data Protection Impact Assessment where the change is narrow — is required before any of the following goes live:

- A new product, service, or material feature that processes customer personal data;
- A new category of personal data, or a new purpose for existing data;
- A new supplier or subcontractor that will access personal data, or a material change in an existing one;
- A material change to systems, hosting, architecture, or access model;
- Entry into a new state or a new customer segment with different regulatory exposure;
- Any Critical or High severity incident, where the assessment forms part of the post-incident review.

12.3 Methodology

Each assessment identifies the risk, the affected data and individuals, the existing controls, and then scores inherent and residual risk on a severity-by-likelihood matrix. Severity considers the sensitivity of the data, the

number of individuals affected, and the potential harm — clinical, financial, reputational, and regulatory. Each risk is assigned a rating of Critical, High, Medium, or Low, and is recorded in the privacy risk register with an owner.

12.4 Output and Reporting

Each assessment produces a written report containing the scope, methodology, findings, the risk register extract with ratings, and a mitigation plan under Section 13. The report is delivered to the CEO and retained for six years. A summary suitable for customer due diligence is made available to customers under NDA on request.

13. Risk Mitigation Plans and Management Review

Identifying a privacy risk without closing it is not compliance. Every risk identified through an assessment, audit, incident, complaint, or customer finding is entered in the privacy risk register and carries a formally documented mitigation plan.

13.1 Required Contents of a Mitigation Plan

Each mitigation plan is written and must record, at minimum:

1. A description of the risk and the assets, data categories, and individuals it affects;
2. The inherent risk rating, and the residual rating expected once mitigation is complete;
3. The specific remediation actions to be taken, stated concretely enough to be verifiable;
4. A single named accountable owner — a person, not a team — and any supporting owners;
5. A target completion date, and interim milestones where remediation exceeds 30 days;
6. The resources, budget, or approvals required;
7. Interim compensating controls to be applied while the risk remains open;
8. The evidence that will be produced to demonstrate closure, and who will verify it;
9. Where a risk is accepted rather than mitigated, the written rationale, the accepting executive, and a mandatory review date.

13.2 Remediation Timelines

Rating	Target Remediation	Review and Escalation
Critical	Immediate containment; full remediation within 30 days	Reviewed by the CEO at initiation and at closure. Reported to the Board or governing body. Compensating controls mandatory until closed.
High	Within 60 days	Reviewed by the CEO and Privacy Officer monthly until closed. Escalated to the CEO if the target date is missed.
Medium	Within 90 days	Reviewed at the quarterly management review. Escalated if it slips two consecutive quarters.
Low	Within 180 days, or accepted with rationale	Reviewed at the quarterly management review.

13.3 Formal Management Review

Mitigation plans are reviewed by management on a defined cadence, and the review is minuted:

- **Quarterly Privacy and Security Management Review.** Chaired by the CEO, attended by the Privacy Officer, Security Officer, and Compliance Officer. The meeting reviews the full risk register, the status of every open mitigation plan against its target date, incidents since the last review, training completion, audit findings, rights request performance, and any proposed risk acceptance. Minutes record the decisions, the risks accepted, and the actions assigned, and are retained for six years.
- **Annual review and sign-off.** The CEO formally reviews and signs the annual privacy risk assessment report and the state of the risk register, confirming that identified risks are either remediated, actively being remediated within timeline, or formally accepted with documented rationale.
- **Board or governing body reporting.** Critical risks, material incidents, and any risk accepted at Critical or High level are reported to the Board or governing body at its next regular meeting.

13.4 Verification of Closure

A mitigation plan is closed only when the accountable owner produces the evidence identified in the plan and the Privacy Officer or Security Officer — someone other than the owner — verifies it. Self-certified closure without independent verification is not permitted. Closure is recorded in the risk register with the date, the verifier, and a reference to the evidence.

13.5 Overdue Items

A mitigation plan that passes its target date without closure is automatically escalated to the CEO with the reason for the delay, the revised date, and the compensating controls in place. Repeated slippage by the same owner is addressed through the performance or contract management process.

14. Suppliers, Subcontractors, and Partners

14.1 Due Diligence Before Engagement

No supplier, subcontractor, or partner receives or accesses personal data until the Contract Owner has completed and documented privacy and security due diligence, comprising at minimum: the categories of data the third party will process and confirmation that they fall within Section 6; confirmation of US-only storage, processing, and support under Section 7.3; review of the third party's security controls and any available independent attestation; review of its incident history and notification commitments; and confirmation of its own subcontracting practices.

14.2 Contractual Requirements

Every third party that processes personal data on TeleHCN's behalf must execute, before any data is shared, an agreement imposing at minimum:

- A Business Associate Agreement where PHI is involved, meeting 45 C.F.R. §§ 164.504(e) and 164.314(a);
- Purpose limitation restricting processing to the services described, with no secondary use;
- The US-only data residency and personnel location restrictions in Section 7.3, flowed down to any onward subcontractor;
- Security requirements no less protective than Section 8;

- Incident notification to TeleHCN within 48 hours of discovery, with cooperation in investigation and notification;
- Confidentiality obligations surviving termination;
- Return or certified destruction of personal data at termination;
- Audit and evidence rights sufficient for TeleHCN to verify compliance;
- Prior written notice and approval before engaging any onward subcontractor.

14.3 Ongoing Oversight

The supplier register records every third party with access to personal data, the categories of data, the processing and support locations, the agreements in force and their dates, and the date of last review. Each third party is reviewed at least annually against the criteria in Section 14.1, and immediately on notification of a material change, an incident, or a change in processing location. A third party that no longer meets the standard is remediated to a documented plan under Section 13 or exited, with data returned or destroyed under Section 9.4.

14.4 Communication of This Policy to Third Parties

This Policy is provided to suppliers, subcontractors, and partners at onboarding and is incorporated by reference into their agreements, so that its requirements are contractually binding rather than advisory. See Section 15.

15. Communication of This Policy

A policy that is not distributed and understood is not a control. TeleHCN communicates this Policy through defined channels to each audience, and records that it has done so.

Audience	How the Policy Is Communicated	Evidence Retained
Employees	Issued during onboarding before any system access is granted; covered in the mandatory onboarding privacy training module; permanently available on the internal policy portal; reinforced in annual refresher training; summarized in periodic awareness communications.	Signed acknowledgment; training completion record; portal access log.
Contracted clinicians and contractors	Attached to and incorporated by reference into the independent contractor agreement; issued with the onboarding pack before credentials are provisioned; covered in the same mandatory training as employees; available on the clinician portal.	Signed acknowledgment; executed contract incorporating the Policy; training completion record.
Suppliers and subcontractors	Provided during procurement due diligence; incorporated by reference into the BAA or services agreement; re-issued at each annual vendor review and on any amendment.	Executed agreement; due diligence file; annual review record.

Audience	How the Policy Is Communicated	Evidence Retained
Partners and customers	Made available on request as part of third-party risk assessment and contracting, under NDA where appropriate; a summary is published at telehealthcarenetwork.com .	Distribution log maintained by the Privacy Officer.
New joiners mid-cycle	Same as their category above, completed before access is granted rather than at the next scheduled cycle.	Onboarding checklist signed by HR/Credentialing.

15.1 Acknowledgment Required

Every person covered by this Policy acknowledges it before receiving access to any system containing personal data, and again at each annual training cycle. Access is not provisioned until the acknowledgment is on file, and HR and Credentialing verify this as a gating step in the onboarding checklist. The acknowledgment is made in one place only, and no person is asked to sign a separate copy of this Policy.

- **Engaged under an agreement with the Company.** Where a person is engaged under a TeleHCN employment agreement, independent contractor agreement, professional services agreement or similar written engagement, the acknowledgment schedule of that agreement is the acknowledgment of this Policy. For clinicians engaged under the TeleHCN Professional Services Agreement for the URM Rochester programme, that is Schedule B. Signing the agreement acknowledges this Policy and the Incident Response Plan in full; nothing further is signed, at engagement or at any annual renewal.
- **Everyone else.** Any person not engaged under such an agreement — including officers, directors, advisors and any person whose engagement document contains no acknowledgment schedule — acknowledges this Policy on a form issued by the Compliance Officer, which captures the same certifications. The Compliance Officer issues that form at engagement and at each annual cycle.
- **Record.** The Compliance Officer records each acknowledgment — the person, the version acknowledged and the date — and retains it for six years under Section 9.1.

15.2 Availability

The current version of this Policy is published at telehealthcarenetwork.com/policies and is available at all times on the internal policy portal and the clinician portal. Superseded versions are archived with their effective and retirement dates so that it is always possible to establish which version was in force at a given time, and the version number and effective date appear on the cover page of every version. Where a contract incorporates this Policy by reference, the version in force at the effective date of that contract is identified in the contract itself.

16. Communicating Changes to This Policy

Changes to this Policy are controlled, versioned, and actively communicated. Silent amendment is prohibited.

16.1 Change Classification

Change Type	Examples	Communication and Timing
Material	New or changed obligations on personnel; changes to data categories, residency, retention, security requirements, or rights processes; changes required by new law.	Approved by the CEO. Direct email notification to all employees, contractors, suppliers, and partners at least 14 days before the effective date, with a summary of what changed and what each audience must do differently. Re-acknowledgment required from employees and contractors. Customers notified where the change affects contracted commitments.
Minor	Clarifications, corrections, updated contact details, formatting, cross-reference fixes.	Approved by the Privacy Officer. Notified in the next scheduled awareness communication and reflected in the version history. No re-acknowledgment required.
Emergency	Change required immediately by a regulator, a court, or an active incident.	Effective on issue. Notified to all affected audiences within 24 hours, with ratification at the next Quarterly Management Review.

16.2 Standard Change Process

1. The Privacy Officer drafts the change and identifies which audiences it affects.
2. The change is reviewed by the Security Officer and the Compliance Officer, and by legal counsel where it responds to a legal development.
3. The CEO approves material changes; the Privacy Officer approves minor changes.
4. The version number and effective date are updated and the version history table is completed.
5. Notification is issued to each affected audience through the channels in Section 15, in the timeframe set by the classification above.
6. Re-acknowledgment is collected where required, and completion is tracked by the Compliance Officer to the same standard as training under Section 18.5.
7. Supplier and partner agreements incorporating the Policy by reference are updated at the next review, or immediately where the change is material.
8. The superseded version is archived; the new version is published to the portals.

16.3 Customer Notification

Where a change affects commitments made to a customer in a BAA or services agreement, the customer is notified in writing before the change takes effect and, where the agreement requires it, the change is made only with the customer's consent.

17. Monitoring Legal Developments and Keeping This Policy Current

Yes — TeleHCN routinely updates this Policy to address changes in data protection law. The mechanism is as follows.

17.1 Scheduled Review

The Privacy Officer conducts a full review of this Policy at least annually, timed to follow the annual privacy risk assessment so that findings feed directly into the revision. The review is recorded in the version history table even where no change results, so that it is always evident when the Policy was last examined.

17.2 Continuous Monitoring

Between scheduled reviews, the Privacy Officer maintains a regulatory watch covering:

- Rulemaking, guidance, enforcement actions, and resolution agreements from the HHS Office for Civil Rights;
- Federal legislative and regulatory developments affecting health privacy, telehealth, and data security;
- State legislative sessions in every state where TeleHCN operates or where its clinicians are licensed, covering health privacy, medical records, breach notification, telehealth, and consumer privacy statutes;
- State attorney general enforcement and guidance;
- Federal Trade Commission enforcement concerning health data and privacy representations;
- Changes in customer contractual requirements and in accreditation or certification standards TeleHCN is asked to meet;
- Material changes in the threat environment relevant to health care.

The watch is supported by subscription to legal and regulatory update services, membership of relevant professional associations, and periodic review by external counsel. Where TeleHCN begins operating in a new state, the Privacy Officer completes a gap assessment against that state's requirements before service begins.

17.3 Trigger-Based Review

A review is initiated within 30 days, irrespective of the annual cycle, on any of the following:

- Enactment or material amendment of a law or regulation applicable to TeleHCN;
- Publication of significant regulatory guidance or a material enforcement action;
- A Critical or High severity incident, or a pattern of lower-severity incidents;
- A finding from an internal audit, customer audit, or regulatory examination;
- A material change in TeleHCN services, systems, suppliers, or geographic footprint;
- Entry into a new state or a new category of customer.

17.4 From Legal Change to Operational Change

Identifying a legal change is not sufficient. Each identified change is logged in the regulatory change register with an assessment of applicability, a gap analysis against current practice, and — where a gap exists — a mitigation plan under Section 13 with a named owner and a target date tied to the statutory compliance deadline. Policy text, training content, contractual templates, and system configuration are updated together, so that the written Policy and the operating practice do not diverge.

17.5 Version History

Version	Effective Date	Approved By	Summary of Changes
1.0	1 January 2026	V. Raina, MD	Initial issue. Adopted 4 October 2026.

Version	Effective Date	Approved By	Summary of Changes

18. Privacy and Data Protection Training

Every person with access to customer personal data — employee and contractor alike — must complete privacy and data protection training before access is granted and at least annually thereafter. The curriculum is set out in the companion document, the **TeleHealthcare Network Privacy and Security Training Curriculum** (the "Curriculum"), which forms part of this Policy and is maintained by the Privacy Officer.

18.1 Who Must Train

Training is mandatory, on identical terms, for: employees; contracted clinicians and all other independent contractors; temporary, locum tenens, and agency personnel; officers and directors with data access; and any supplier personnel embedded in TeleHCN operations with direct system access. Suppliers who process data on their own systems must certify annually that their personnel receive equivalent training.

18.2 Onboarding Training — Before Access

Privacy training is completed at onboarding and before the individual receives access to any system containing customer personal data. Access provisioning is gated: HR and Credentialing will not submit an access request, and the Security Officer will not provision credentials, until the training completion record and the required Policy acknowledgment are on file — which, for a person engaged under a TeleHCN agreement, is the acknowledgment schedule of that agreement, signed once at engagement and not re-signed at completion or at any annual renewal, and for anyone else is the form issued by the Compliance Officer under Section 15.1. There is no provisional or temporary access pending training.

Onboarding training covers the Curriculum's core modules and must be completed within the first five business days of engagement, or earlier where the individual is scheduled for clinical coverage sooner.

18.3 Annual Refresher Training

All personnel complete refresher training at least once every 12 months, within a 30-day completion window opened by the Compliance Officer. The refresher covers changes to this Policy, changes in law identified under Section 17, lessons from incidents in the preceding year, and any area where monitoring under Section 19 has identified weakness. Role-specific supplementary training is assigned to those with elevated access, credentialing responsibilities, or incident response duties.

18.4 Event-Driven Training

Additional training is assigned when: this Policy changes materially; an individual changes role or receives expanded access; an individual is involved in a privacy incident or policy violation; monitoring identifies a knowledge gap; or a new system, service, or data category is introduced.

18.5 Completion Requirements, Tracking, and Consequences

- **Completion standard.** Training is complete only when the individual has finished all assigned modules, passed the assessment at 80% or above, and signed the acknowledgment. Two reattempts are permitted; a third failure requires supervised remediation before access continues.
- **Tracking.** The Compliance Officer maintains a training register recording, for every individual: name, role, employment or contract status, modules assigned, date assigned, date completed, assessment score, acknowledgment date, and next due date. Records are retained for six years under Section 9.1.
- **Monitoring.** Completion is reviewed monthly by the Compliance Officer and reported at the Quarterly Management Review, broken out separately for employees and contractors. The target is 100% completion within the window.
- **Reminders.** Automated reminders are issued at 14 days, 7 days, and 1 day before the deadline, and daily thereafter, with the individual's manager or clinical lead copied from the deadline onward.

Consequences of Non-Completion

Status	Consequence — Employees	Consequence — Contracted Clinicians and Contractors
Deadline missed (1–7 days overdue)	Written reminder; manager notified; completion required within 7 days.	Written reminder; clinical lead and scheduling notified; completion required within 7 days.
8–14 days overdue	Formal written warning placed on file. Access to systems containing personal data suspended until completion.	Access suspended. Removed from the scheduling roster for future shifts until completion. Notice recorded in the contractor file.
More than 14 days overdue	Access remains suspended. Escalation to the CEO. Progressive discipline up to and including termination of employment.	Access remains suspended. No further shifts assigned. Escalation to the CEO. Grounds for termination or non-renewal of the contract for breach.
Failure to complete after suspension	Termination of employment.	Termination of the contract. Removal from the approved clinician roster.

Suspension of access for non-completion is applied automatically by the Security Officer on notification from the Compliance Officer, and is not subject to managerial discretion or business-need override.

18.6 Evidence for Customers

On request from a customer conducting third-party risk assessment, TeleHCN provides aggregate training completion statistics, the current Curriculum, and — where the customer agreement provides for it — confirmation that the specific clinicians assigned to that customer have current training.

19. Monitoring, Auditing, and Enforcement

TeleHCN operates a defined process for monitoring compliance with this Policy and enforcing it. Compliance is verified, not assumed.

19.1 Continuous Technical Monitoring

- Access to systems containing personal data is logged at the record level where supported, and logs are protected against alteration and retained for six years;
- Automated alerting flags anomalous access patterns — access outside normal hours or role profile, high-volume record access, access to records of individuals sharing a surname or address with the user, access from an unexpected location or unrecognized device, and repeated failed authentication;
- Data loss prevention controls monitor for unauthorized export, download, printing, or transmission of personal data;
- Geographic access controls under Section 7.2 alert or block on any access attempt from outside the United States;
- Endpoint management reports on encryption status, patch level, and protection status for every device permitted to access personal data.

19.2 Scheduled Audits and Reviews

Activity	Frequency	Owner and Output
User access review and recertification	Quarterly	Security Officer with system owners. Attestation that each user's access remains appropriate; removal of unnecessary access.
Access log review — targeted sampling	Monthly	Compliance Officer. Sample of high-risk access reviewed against a documented business justification.
Policy compliance audit	Annually	Compliance Officer. Tests a sample of controls across all sections of this Policy; findings entered in the risk register.
Privacy risk assessment	Annually	Privacy Officer. Section 12.
Supplier and subcontractor review	Annually	Contract Owners. Section 14.3.
Retention and destruction verification	Annually	Privacy Officer. Confirms destruction occurred on schedule; certificates on file.
Incident response tabletop exercise	Annually	Security Officer. Documented results feed plan updates.
Training completion review	Monthly	Compliance Officer. Section 18.5.
Management review of risk and mitigation	Quarterly	CEO. Section 13.3.

19.3 Investigation

Suspected violations are investigated by the Compliance Officer, with the Privacy Officer and Security Officer as required. Everyone must cooperate fully and answer truthfully. Access may be suspended during investigation as a protective measure; suspension is not itself a disciplinary finding. Destroying, altering, or

concealing evidence, or discouraging another person from reporting or cooperating, is a serious violation in its own right.

19.4 Sanctions

Sanctions are applied consistently, proportionately, and identically to employees and contractors, taking into account the sensitivity of the data, the harm caused, whether the conduct was intentional, whether it was self-reported, and prior history.

Conduct	Sanction
Inadvertent minor violation, promptly self-reported, no harm	Coaching and targeted retraining. Recorded but not disciplinary.
Negligent violation, or repeated minor violations	Written warning, mandatory retraining, and increased monitoring. For contractors, a written notice recorded in the contractor file.
Serious violation — unauthorized access, prohibited data handling, failure to report an incident within 24 hours	Final written warning, suspension of access, and possible termination. For contractors, immediate removal from assignment and possible termination of contract.
Intentional misuse — snooping, disclosure for personal gain, access from outside the United States, circumvention of security controls, retaliation against a reporter	Immediate termination of employment or contract. Referral to licensing boards where a clinician is involved, and to law enforcement where the conduct may be criminal. Removal from the approved clinician roster.
Falsifying training completion, audit evidence, or an investigation response	Immediate termination of employment or contract.

Sanctions applied are recorded by the Compliance Officer and retained for six years. Aggregate sanction data is reported at the Quarterly Management Review.

19.5 Reporting and Non-Retaliation

Anyone may report a suspected violation to the Privacy Officer, the Security Officer, the Compliance Officer, or any member of executive leadership. TeleHCN prohibits retaliation against any person who reports in good faith, refuses to participate in conduct they reasonably believe unlawful, or cooperates in an investigation. Nothing in this Policy limits any person's right to report a possible violation of law to a government agency, to participate in an agency investigation, or to receive a whistleblower award, without prior authorization from or notice to TeleHCN.

19.6 Exceptions

Any exception to this Policy requires written approval from the Privacy Officer and the Security Officer, must record the business justification, the compensating controls, the accountable owner, and an expiry date not exceeding 12 months, and is entered in the exceptions register. Exceptions are reviewed at each Quarterly Management Review and expire automatically unless renewed. There are no exceptions to Section 7 (data residency) or to the prohibited practices in Section 8.4.

20. Related Documents and Review

20.1 Related Documents

- TeleHealthcare Network Code of Conduct and Ethics Policy
- TeleHealthcare Network Notice of Privacy Practices
- TeleHealthcare Network Privacy and Security Training Curriculum
- TeleHealthcare Network Record of Processing Activities (Section 4.6 of this Policy)
- Incident Response Plan
- Data Retention Schedule (Section 9.1 of this Policy)
- Business Associate Agreement template and Subcontractor Agreement template
- Access Control Standard and Acceptable Use Standard
- Supplier Register, Privacy Risk Register, Exceptions Register, Rights Request Register, Incident Register, Training Register

20.2 Policy Review

This Policy is reviewed at least annually by the Privacy Officer and approved by the Chief Executive Officer, and is reviewed on any trigger listed in Section 17.3. The date of each review is recorded in the version history at Section 17.5 whether or not the Policy is amended.

20.3 Questions

Questions about this Policy, and requests for guidance on a situation it does not clearly address, should be directed to the Privacy Officer before acting. Asking first is always the correct course.