



TeleHealthcare
Network

Augmenting Care Through Virtual Coverage

PRIVACY AND SECURITY TRAINING CURRICULUM

TELEHEALTHCARE NETWORK

Mandatory training for all employees and contracted clinicians
with access to customer or patient personal data

Version 1.0

Effective Date: 1 January 2026

Date Adopted: 4 October 2026

Curriculum Owner: Vimarsh Raina, MD — Privacy Officer

Approved by: Vimarsh Raina, MD — Chief Executive Officer

Companion to the TeleHCN Privacy and Data Protection Policy

Review Cycle: Annually, and upon material change to law or policy

1. Purpose and Standing

This Curriculum is the training program referenced at Section 18 of the TeleHealthcare Network Privacy and Data Protection Policy (the "Policy"). It forms part of that Policy. It specifies what TeleHCN teaches, to whom, when, how completion is measured, how records are kept, and what happens when training is not completed.

The Curriculum exists so that the training commitment in the Policy points to something real and auditable. A customer conducting third-party risk assessment, or a regulator examining the privacy program, should be able to read this document and know exactly what every person with access to their data was taught and when.

1.1 Learning Objectives

On completing this program, every participant will be able to:

1. Identify what constitutes personal data and protected health information in the TeleHCN context, and recognize it when they encounter it.
2. Apply the minimum necessary standard to a real access decision, and explain why a given access was justified.
3. State the rules on where they may work from, what devices and tools they may use, and what they may never do with personal data.
4. Recognize a privacy or security incident, including ones that do not look like incidents, and report it within 24 hours through the correct channel.
5. Handle a request from a patient or customer to exercise a privacy right, and route it correctly rather than answering it themselves.
6. Describe the consequences — for the patient, for the customer, for TeleHCN, and for themselves — of failing to meet these obligations.

1.2 Who to Contact

Questions about this Curriculum, requests for a live question-and-answer session, and requests for aggregate completion evidence should be directed to the Privacy Officer. Technical questions about access provisioning, devices, and approved tools should be directed to the Security Officer.

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

2. Who Must Complete It

Training obligations are identical for employees and contractors. Contractor status does not reduce the requirement, extend the deadline, or soften the consequence of non-completion.

Population	Onboarding	Annual Refresher	Role-Specific Modules
Employees — all roles with data access	Required before access	Required	By role
Contracted clinicians (MD, DO, NP, PA)	Required before access	Required	Clinical module required
Independent contractors — non-clinical	Required before access	Required	By role
Temporary, locum tenens, agency personnel	Required before access	Required if engagement exceeds 12 months	By role
Officers and directors with data access	Required before access	Required	Governance module
Privacy, Security, Compliance Officers	Required before access	Required	Advanced modules M8–M10
Credentialing and HR staff	Required before access	Required	M9 (workforce data)
Embedded supplier personnel with direct system access	Required before access	Required	By role
Suppliers processing data on their own systems	Annual written certification of equivalent training	—	—

Access Is Gated on Completion

No individual receives credentials to any system containing customer or patient personal data until the training completion record and the required Policy acknowledgment are on file — for a contractor, the acknowledgment schedule of their engagement agreement; for anyone else, the form issued by the Compliance Officer. HR and Credentialing verify this as a gating step in the onboarding checklist; the Security Officer will not provision access without it.

There is no provisional access, no temporary access pending training, and no business-need override. A clinician who has not completed training cannot be scheduled for a shift.

3. Curriculum Structure

The program comprises seven core modules required of everyone, and four role-specific modules assigned by access profile. Core modules total approximately 90 minutes at onboarding and approximately 50 minutes at annual refresh.

3.1 Core Modules — Required of All Personnel

Ref	Module	Content Covered	Duration
M1	Why This Matters	What TeleHCN does and whose data it touches. Real consequences of privacy failure: harm to patients in small communities where re-identification is easy; OCR enforcement and civil monetary penalties; loss of customer contracts; individual criminal liability under HIPAA. Framing: the record belongs to the patient, not to us. Policy §1, §5.	10 min
M2	What Counts as Personal Data	PHI and the 18 HIPAA identifiers. Customer personal data, workforce data, business contact data. De-identification and why "it looked anonymous" is not a defence. Categories TeleHCN permits, restricts, and prohibits, and what to do when prohibited data arrives unsolicited. Policy §2.2, §6.	12 min
M3	Minimum Necessary in Practice	The minimum necessary standard and its exceptions. Worked scenarios: which records may I open on this shift; how much of the chart is relevant; when may I look at a record for a patient I am not covering. Prohibition on curiosity access — coworkers, family, neighbours, public figures, self. Access in place rather than copying. Policy §5.1, §5.2.	15 min
M4	Working Securely, and Where You May Work From	The United States-only requirement and what it means in practice: no access from abroad, ever, including while travelling or on holiday; VPN and location-masking treated as intentional circumvention. Approved platforms and devices; prohibited tools including personal email, SMS, consumer messaging, and unapproved AI or transcription services. Passwords, MFA, credential sharing, screen locking, physical privacy during remote shifts. Policy §7, §8.2, §8.4.	18 min
M5	Recognizing and Reporting Incidents	What an incident looks like, including the ones that do not feel like incidents: a misdirected email, a lost phone, a chart left open, a colleague using your login. The 24-hour reporting duty. How and to whom to report. Why self-reporting is protected and concealment is not. Phishing recognition exercise. Policy §11.	15 min
M6	Individual Rights and Requests	The rights individuals hold: access, correction, deletion, portability, restriction, objection, confidential communications, accounting of disclosures. Why you must never answer a rights request yourself. How to route a request to the Privacy Officer within the deadline. The mandatory out-of-pocket restriction. Policy §10.	10 min
M7	Rules, Monitoring, and Consequences	What is monitored and logged, and that every access is attributable to one person. The audit and sampling program. The sanctions table and how it is applied identically to employees and contractors. Non-retaliation and protected government disclosures. Where to ask	10 min

Ref	Module	Content Covered	Duration
		when unsure. Policy §19.	

3.2 Role-Specific Modules

Ref	Module	Assigned To / Content	Duration
M8	Clinical Practice and Privacy	All contracted clinicians. Documentation integrity and prohibition on cloned or fabricated notes. Discussing patients with facility staff and families. 42 C.F.R. Part 2, behavioural health, HIV, and reproductive health records. Handoff and escalation without over-disclosure. Facility-specific rules and where they are stricter than ours.	20 min
M9	Workforce and Credentialing Data	HR, Credentialing, Finance. Handling licensure, background check, malpractice, tax, and payment data. Field-level access limits. Retention and destruction of applicant and clinician files. Exclusion screening data.	15 min
M10	Third Parties and Contracting	Contract Owners, procurement, business development. Due diligence before data is shared. BAA and subcontractor agreement requirements. Verifying US-only storage, processing, and support. Annual vendor review. What to do when a supplier reports an incident.	20 min
M11	Incident Response for Responders	Privacy, Security, Compliance Officers and their delegates. Severity classification. Containment. Breach risk assessment under the four §164.402 factors. Notification deadlines to customers, individuals, OCR, and state authorities. Evidence preservation and legal hold. Post-incident review.	45 min

4. Delivery, Timing, and Cadence

4.1 Onboarding

Core modules M1–M7 plus any assigned role-specific module are completed before system access is provisioned, and in any event within the first five business days of engagement — earlier where the individual is scheduled for clinical coverage sooner. Onboarding training is delivered through the learning platform with a live question-and-answer session available on request from the Privacy Officer.

4.2 Annual Refresher

All personnel complete a refresher at least once every 12 months. The Compliance Officer opens a 30-day completion window and notifies participants at the start. The refresher is not a replay of the onboarding material; it is rebuilt each year to cover:

- Changes to the Policy since the last cycle, and what each audience must now do differently;
- Changes in federal and state law identified through the regulatory watch at Policy §17;
- Anonymized lessons from incidents at TeleHCN in the preceding 12 months;

- Findings from the annual privacy risk assessment and the compliance audit;
- Any area where access log review or monitoring identified a recurring weakness;
- Refreshed phishing and social engineering recognition.

4.3 Event-Driven Training

Additional training is assigned, outside the annual cycle, when:

Trigger	Assigned To	Deadline
Material amendment to the Privacy and Data Protection Policy	All affected personnel	30 days from effective date
Role change or expansion of data access	The individual	Before expanded access is provisioned
Involvement in a privacy incident or policy violation	The individual, and their team where systemic	14 days from incident closure
Monitoring or audit identifies a knowledge gap	The affected group	30 days from finding
New system, service, or data category introduced	Users of that system or data	Before access is granted
New state of operation with differing requirements	Clinicians licensed in that state	Before service begins

4.4 Delivery Methods

- Primary delivery through the TeleHCN learning management system, accessible on demand, with progress saved between sessions;
- Live or recorded briefings for material policy changes and for the incident responder module;
- Scenario-based exercises drawn from real telehealth situations rather than generic examples;
- Simulated phishing campaigns at least quarterly, with immediate targeted micro-training for anyone who engages with a simulation;
- Periodic awareness communications between formal cycles — short, specific, and tied to something that actually happened.

5. Assessment and Completion Standard

5.1 What Counts as Complete

Training is recorded as complete only when all three of the following are satisfied:

1. All assigned modules have been worked through in full, with the platform recording time in module;
2. The end-of-course assessment has been passed at 80% or above;
3. The required acknowledgment is on file. For a person engaged under a TeleHCN agreement this is the acknowledgment schedule of that agreement (for the URM Rochester programme, Schedule B), which is signed once and is accepted in place of any separate form — nothing further is signed at completion or

at any annual renewal. For anyone else it is the acknowledgment form issued by the Compliance Officer under Policy §15.1.

Partial completion is not completion. Watching the material without passing the assessment does not satisfy the requirement and does not unlock access.

5.2 Assessment Design

- Minimum 20 questions for the core program, drawn from a larger pool so that reattempts are not identical;
- Scenario-based rather than definitional — participants are asked what they would do, not what a term means;
- Every question maps to a stated learning objective at Section 1.1 and to a Policy section;
- Pass mark 80%. Feedback is given on incorrect answers with a reference to the governing Policy section.

5.3 Reattempts

Two reattempts are permitted. A third failure requires supervised remediation with the Privacy Officer before the individual continues to hold access; where the individual already holds access, access is suspended pending remediation.

5.4 Attestations Collected

For contractors engaged under a TeleHCN professional services agreement, every attestation below is captured by the acknowledgment schedule in that agreement (for the URMCH Rochester programme, Schedule B) and none is collected again at completion. The contractor signs once, at contracting. For employees and others not engaged under such an agreement, the attestations are signed at each completion. In either case TeleHCN retains:

- Acknowledgment that they have read and will comply with the Privacy and Data Protection Policy;
- Attestation that they will access TeleHCN and customer systems only from within the United States, at all times and including while travelling;
- Confirmation that they understand the 24-hour incident reporting duty;
- Confirmation that they understand access is monitored and logged, and that violations carry the sanctions at Policy §19.4.

6. Tracking and Records

6.1 The Training Register

The Compliance Officer maintains a training register recording, for every individual subject to this Curriculum:

Field	Purpose
Name, role, and employment or contract status	Enables reporting broken out separately for employees and contractors.
Access profile and systems held	Determines which role-specific modules are assigned.
Modules assigned and date assigned	Establishes the obligation and starts the clock.

Field	Purpose
Date completed and time in module	Evidence of actual participation, not merely enrolment.
Assessment score and number of attempts	Evidence the completion standard was met.
Acknowledgment and attestation dates	Links training to the signed commitments in Section 5.4.
Next due date	Drives the reminder schedule and the overdue report.
Overdue status and actions taken	Evidence that consequences were applied consistently.
Access suspension and reinstatement dates	Demonstrates the gating control operates.

Training records are retained for six years in accordance with 45 C.F.R. § 164.530(j) and Policy §9.1.

6.2 Reminders

Automated reminders are issued at 14 days, 7 days, and 1 day before the deadline, and daily thereafter. From the deadline onward the individual's manager or clinical lead is copied on every reminder.

6.3 Reporting

- The Compliance Officer reviews completion monthly and issues an overdue report to managers and clinical leads;
- Completion is reported at each Quarterly Privacy and Security Management Review, broken out separately for employees and contractors, with the target stated as 100% within the completion window;
- Any individual more than 14 days overdue is named in the report to the CEO;
- Aggregate completion statistics are provided to customers on request as part of third-party risk assessment, and where a customer agreement provides for it, confirmation that the specific clinicians assigned to that customer hold current training.

7. Consequences of Non-Completion

Consequences are stated in advance, applied automatically, and applied identically to employees and contractors. Suspension of access for non-completion is applied by the Security Officer on notification from the Compliance Officer and is not subject to managerial discretion or business-need override.

Status	Employees	Contracted Clinicians and Contractors
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.

Status	Employees	Contracted Clinicians and Contractors
8–14 days overdue	Formal written warning 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. Escalated to the CEO. Progressive discipline up to and including termination of employment.	Access remains suspended. No further shifts assigned. Escalated to the CEO. Grounds for termination or non-renewal for breach of contract.
Failure to complete after suspension	Termination of employment.	Termination of contract. Removal from the approved clinician roster.
Falsifying completion or assessment results	Immediate termination of employment.	Immediate termination of contract. Removal from the approved clinician roster.

Time lost to suspension is not compensable, and shifts released because a clinician was suspended for non-completion are treated as clinician-initiated cancellations under the applicable contract.

8. Curriculum Maintenance and Effectiveness

8.1 Annual Review

The Privacy Officer reviews and updates this Curriculum at least annually, timed to follow the annual privacy risk assessment so that findings feed the next cycle's content. The review date is recorded at Section 9 whether or not content changes.

8.2 Trigger-Based Update

Content is updated within 30 days of: a material amendment to the Policy; a change in applicable law identified through the regulatory watch; a Critical or High severity incident; an audit or customer finding; or introduction of a new system, service, or data category.

8.3 Measuring Whether It Works

Training is assessed on outcomes, not on completion rate alone. The following are reviewed at each Quarterly Management Review, and a sustained adverse trend generates a mitigation plan under Policy §13:

- Completion rate within the window, employees and contractors reported separately;
- First-attempt assessment pass rate, and the questions most frequently answered incorrectly;
- Phishing simulation engagement rate and trend;
- Number of incidents attributable to human error, and whether the underlying behaviour was covered in training;
- Incident reporting latency — the proportion reported within 24 hours;
- Findings from access log sampling that indicate a misunderstanding rather than misconduct.

8.4 Version History

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



**TeleHealthcare
Network**
Augmenting Care Through Virtual Coverage

TRAINING COMPLETION RECORD

Internal record — completed and filed by TeleHCN

This record is completed by TeleHCN and filed in the training register. The participant is not asked to sign it. Persons engaged under a TeleHCN agreement make all required attestations once, in the acknowledgment schedule of that agreement (for the URMCH Rochester programme, Schedule B); anyone else uses the acknowledgment form issued by the Compliance Officer under Policy §15.1.

Participant

Printed Name

Role / Title

Employee or Contractor (circle one)

Primary Work Location (City, State)

Training Completed

The participant completed the TeleHCN Privacy and Security Training — all core modules and any assigned role-specific module, as described in Section 3 of the Curriculum — and passed the assessment at 80% or above.

Curriculum version	Date completed	Assessment score	Attempts
_____	_____	_____	_____

Role-specific module(s) assigned, if any: _____

Acknowledgment on file: _____

The participant's policy acknowledgment is held separately and is not re-collected at completion. Record where it is held — for example the engagement agreement and its date, or the acknowledgment form and its date.

Completion Verified By

Verified By (Name and Title)

Date Verified

Access Provisioned By

Next Refresher Due