



TeleHealthcare
Network

Augmenting Care Through Virtual Coverage

INCIDENT RESPONSE SUMMARY

TELEHEALTHCARE NETWORK

How TeleHealthcare Network detects, contains and reports a suspected breach
of confidential or personal data — public summary

Version 1.0

Effective Date: 1 January 2026

Date Adopted: 4 October 2026

Summary of the TeleHCN Incident Response Plan §§1–14

Full plan available to contracted personnel and to customers on request

1. What This Document Is

TeleHealthcare Network maintains a documented Incident Response Plan governed by Section 11 of the TeleHCN Privacy and Data Protection Policy. This is a public summary of that plan. It states what a clinician, a customer or a patient needs to know about how TeleHCN responds when data may have been compromised.

The full plan is not published, because it records detection thresholds, escalation timings, containment authorities and contact details whose disclosure would assist anyone attempting to attack TeleHCN or its customers. It is provided in full to every contracted clinician and employee at onboarding, and to customers and prospective customers on request under an appropriate confidentiality agreement.

If You Think Something Has Gone Wrong

Report it within 24 hours to the Privacy Officer or the Security Officer, using the contacts in Section 7. You do not need to be sure, you do not need to investigate first, and you do not need to know whether any data was actually taken.

Reporting in good faith is protected, including when you caused the incident yourself. Failing to report, or delaying a report, is treated more seriously than the underlying mistake.

2. Governance

Incident response has named owners with defined authority, so that nobody has to work out who decides while an incident is live.

Role	Holder	Responsibility
Incident Commander	Security Officer	Leads the response. Triage, severity, containment, technical investigation, evidence preservation, recovery. May suspend accounts, isolate systems and wipe devices without prior approval.
Privacy Lead	Privacy Officer	Determines whether an incident is a reportable breach. Approves the content and timing of every notification to customers, individuals and regulators.
Executive Sponsor	Chief Executive Officer	Accountable for the response. Authorises outside counsel and forensics. Approves external communications.

3. How Incidents Are Detected

TeleHCN relies on both automated controls and human reporting, because each catches what the other misses.

3.1 Automated

- Record-level logging of access to systems containing personal data, retained six years and protected against alteration;
- Alerting on anomalous access — outside normal hours or role, unusually high volume, records of individuals sharing a surname or address with the user, unexpected location or unrecognised device, repeated failed authentication;
- Blocking and alerting on any access attempt from outside the United States;
- Monitoring for unauthorised export, download, printing or transmission of personal data;
- Endpoint detection and response, identity provider monitoring, vulnerability scanning, and backup integrity monitoring.

3.2 Human

- A 24-hour reporting duty binding every employee and contracted clinician, taught in the mandatory training programme;
- Reports from customer facilities and from suppliers, who are contractually required to notify TeleHCN within 48 hours of their own discovery;
- Monthly sampling of access logs, which surfaces incidents that generated no alert;
- Reports from patients, researchers, regulators and law enforcement, which are treated as confirmed until disproved.

4. How TeleHCN Responds

1. Report and log. Every report is recorded on receipt with the date of discovery, because statutory notification deadlines run from discovery rather than from the end of the investigation.
2. Triage and classify. Severity is assigned within 24 hours across four levels. A Critical incident convenes the response team within one hour and engages the Chief Executive Officer and outside counsel immediately.
3. Contain. Stopping ongoing exposure takes priority over investigation and over service continuity. Where containment would affect active clinical coverage, replacement cover is arranged in parallel rather than traded against it.
4. Investigate. Evidence is preserved before any remediation. The investigation establishes what data was involved, whether it was actually accessed or merely exposed, who is affected, and the underlying cause.
5. Assess. Any impermissible use or disclosure of protected health information is presumed to be a breach unless a documented four-factor assessment under 45 C.F.R. §164.402, signed by the Privacy Officer, shows a low probability of compromise.
6. Notify. On the deadlines in Section 5.
7. Recover and review. Verified eradication, restoration from clean backups, then a written post-incident report within 15 business days with corrective actions tracked to completion.

5. Notification

Notification obligations run in parallel, not in sequence. TeleHCN does not wait for investigative certainty before making the first customer notification.

Recipient	Deadline	Notes
Affected customer facility	Per the executed Business Associate Agreement; absent a stated period, no later than 5 calendar days from discovery	States what is known, what is not yet known, what has been contained, and when the next update follows.
Affected individuals	No later than 60 calendar days from discovery	Where TeleHCN is the covered entity. Where TeleHCN is a business associate, the customer notifies and TeleHCN supplies everything the customer needs to meet its own deadline.
HHS Office for Civil Rights	60 days for breaches affecting 500 or more; annually for smaller breaches	In accordance with 45 C.F.R. §164.408.
State attorneys general	Per the law of each affected individual's state of residence — as short as 30 days	Determined by where affected individuals live, not where TeleHCN or the facility is located.
Law enforcement	As soon as criminal conduct is suspected	On the Chief Executive Officer's authorisation.

All notifications, and the date and method of each, are retained for six years as evidence of timeliness.

6. Raising a Privacy Concern or Complaint

Anyone — a patient, a clinician, a customer or a member of the public — may raise a privacy inquiry or complaint with TeleHCN using the contacts in Section 7.

- Every inquiry and complaint is logged on receipt and acknowledged within 5 business days;
- A substantive written response follows within 30 calendar days, stating what was found, what was done and what will change. Where more time is needed you are told before the deadline, with the reason and a revised date;
- Where a complaint is upheld, the corrective action is tracked to verified completion;
- If you are dissatisfied you may escalate in writing to the Chief Executive Officer for independent review;
- You may also complain to the customer facility as covered entity, to your state attorney general, and to the HHS Office for Civil Rights at www.hhs.gov/ocr/privacy/hipaa/complaints/ or 1-877-696-6775. TeleHCN places no condition on your doing so;
- No one is penalised, denied care or treated differently for raising a concern in good faith.

7. Who to Contact

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

7.1 Related Documents

The following are published at telehealthcarenetwork.com/policies: the TeleHCN Code of Conduct and Ethics Policy, the Privacy and Data Protection Policy, the Privacy and Security Training Curriculum, and the Notice of Privacy Practices.

The following are available on request, to contracted personnel and to customers under an appropriate confidentiality agreement: the full Incident Response Plan, the Record of Processing Activities including documented data flows, the System and Supplier Register, and data residency evidence.

This summary is reviewed annually, and after any Critical or High severity incident, alongside the Incident Response Plan it summarises. Where this summary and the full plan differ, the full plan controls.