# TN-500 — HMIS Security Breach Procedure

Approved by: TN-500 Governance Council
Version: 1.0
Last Edited: 11/17/2025

**Applies to:** All TN-500 CoC participating agencies, contractors, volunteers, interns, and staff who access, collect, process, store, transmit, or maintain HMIS or client PII/PHI data.

**Current HMIS Lead:** Chattanooga Regional Homeless Coalition — primary point for reporting, containment, investigation, remediation, and CoC-level communications.

## 1. Purpose

To ensure a rapid, coordinated, lawful, and well-documented response to any suspected or confirmed security breach affecting HMIS or other CoC-held personal information — minimizing harm to clients and the CoC while meeting applicable legal and funder obligations. HUD requires CoCs to have a breach response process; this document operationalizes that obligation for TN-500.

## 2. Definitions

- **Security Breach / Incident:** any confirmed or suspected unauthorized acquisition, access, use, disclosure, loss, destruction, or alteration of HMIS data (including paper records) that compromises confidentiality, integrity, or availability of PII/PHI.
- **PII (Personally Identifiable Information):** e.g., names combined with SSN, DOB, driver's license number, financial account with access codes, or any data defined by state/federal law.
- **PHI:** protected health information under HIPAA when applicable (medical/behavioral health items).
- **Affected Individual(s):** any client, staff, contractor whose personal information was or may have been accessed or acquired by an unauthorized person.

## 3. Breach Severity / Classification (quick triage)

Use this to prioritize response and notifications.

- **Level 1 — Suspected/Low-risk incident:** single account briefly accessed without authorization, no evidence PII/PHI was exfiltrated or compromised, contained immediately.
- **Level 2 — Confirmed moderate-risk incident:** unauthorized access to identifiable client records, limited number of records (e.g., <100 records), or credentials compromised.
- **Level 3 — Confirmed high-risk / large-scale incident:** incidents involving malicious actor intent, unauthorized removal or exposure of sensitive data, public posting of PII/PHI, ransomware disrupting HMIS operations, or large data exfiltration (e.g., >100 records). *(All incidents must be reported internally immediately, using the Agency Incident Report; severity guides external notifications and escalation.)*

**4. Roles & Responsibilities**

- **Reporting Staff / Agency Contact:** Any staff who discovers/suspects an incident must immediately report using the Agency Incident Report (Appendix B) to:
    - Their Agency Security Officer (or Director), **and**
    - TN-500 HMIS Lead Email: **[hmisbreach@homelesscoalition.org]**
- **Agency Security Officer (or Director):** Performs immediate containment steps for agency systems, preserves evidence, notifies HMIS Lead if not already done, and coordinates with IT/cyber partners.
- **HMIS Lead (Chattanooga Regional Homeless Coalition):** Acts as the central incident coordinator. The HMIS Lead provides containment guidance,-serves as the investigative lead, sends cross-agency notifications, logs and maintains incident record, coordinates with legal counsel, and manages external notifications per law/funder requirements.
- **CoC Governance Council / HMIS Committee:** Provides oversight over the entirety of the HMIS system, including HMIS Security Breach actions by the HMIS Lead.

**5. Immediate Response Checklist (first 24 hours)**

1. **Report immediately:** Any staff who discovers an incident MUST report it to their Agency Security Officer (or Director) and the HMIS Lead *immediately* (same day) and complete the Agency Incident Report Form (Appendix B).
2. **Contain:** If possible and safe, Agency Leadership and the HMIS Lead Agency must:
    - Immediately disable compromised user accounts and change passwords / revoke tokens.
    - Immediately isolate affected devices/systems (take offline if necessary).
    - Preserve logs, forensic images, email headers, access records and relevant physical evidence (do NOT alter evidence).
    - If ransomware, do not power down systems unless advised by forensics — preserve image.
3. **Assess scope:** HMIS Lead with Agency IT/forensics to determine what data and how many records may be affected (estimated scope within 24–72 hours).
4. **Law enforcement:** If criminal activity suspected (e.g., ransomware, extortion, unauthorized access by outsider), immediately notify local law enforcement and coordinate on timing for notifications (law enforcement may request notification delays).
5. **Notify internal governance:** HMIS Lead notifies HMIS Committee and CoC Governance Council Executive leadership within 24 hours of discovery.

## 6. Notifications

### A. Law enforcement

- **As soon as suspected criminal activity is identified,** coordinate with law enforcement on public notification timing if requested.

### B. Affected individuals (clients/staff)

- **Tennessee law:** Any Tennessee resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person must be notified no later than **45 days** after discovery, unless law enforcement requires a delay. If an agency or user maintains data on behalf of another entity, the data owner/licensee must be notified within 45 days. **Therefore:** prepare and send individual notifications *as soon as the scope*

*is determined and notification content is approved*, and always within the 45-day statutory window unless formally delayed by law enforcement (via a written document or an email from a Law Enforcement Official's email address).

- Notifications should include what happened (brief), the information involved, steps the CoC is taking to rectify the breach, recommended actions recipients can take to protect themselves, who to contact for questions, and resources for protection.

**C. Attorney General / State agencies**

- **If >1,000 Tennessee residents are affected** (or as statute requires), notify the Tennessee Attorney General / main regulator as required by state law. (Seek guidance from HMIS Lead and TN-500 Governance Council; consult legal counsel.)

**D. Funding agencies / HUD**

- HUD does not publish a single CoC-level breach-reporting timeline, but HUD Exchange guidance and HUD incident SOPs stress having a process and coordinating with legal counsel. If HUD-funded systems or HUD program data are materially affected, HMIS Lead should coordinate with the Collaborative Applicant (currently the CRHC in both cases), the TN-500 Governance Council, and legal counsel about whether to notify HUD and what information to provide. (If the incident implicates broader HUD systems or significant cybersecurity issues with federal programs, separate HUD reporting requirements may apply to certain partners. Consult HUD guidance/legal counsel.)

**F. Third parties / vendors**

- Notify any vendor, partner, or data owner whose data is implicated immediately (per contract terms).

**7. Remediation & Root Cause / Corrective Action**

- After investigation, the HMIS Lead and affected agency must prepare a written remediation plan within **30 days** of incident confirmation (or sooner depending on severity) and provide it to the Governance Council Executive leadership. The plan must include:
    - Root cause analysis summary.

    - Technical fixes applied (patches, password resets, MFA enforced, revoked credentials).
    - Policy/process changes (e.g., new training, revised account provisioning).
    - Timeline for full remediation and validation.
    - Responsible persons and follow-up reporting timeline.
- Affected agencies must implement corrective actions and confirm completion to HMIS Lead and the Governance Council Executive leadership.

**8. Documentation & Recordkeeping**

- HMIS Lead will maintain the official incident file for at least **7 years** (or as required by funder/state retention rules) including: report forms, investigation notes, forensic reports, notifications, communications, remediation actions, and lessons learned.

**9. Sanctions & Enforcement**

- Failure to report a known or suspected breach, or willful noncompliance with this procedure, may result in administrative action up to suspension of HMIS access, retraining requirements, loss of funding, and/or termination of HMIS Participating Agency Agreement. Specific enforcement procedures will be handled by the CoC Lead following the HMIS Policies & Procedures enforcement processes.

**10. Training & Prevention**

- All HMIS users must complete mandatory privacy & security training at hire and annually.

**11. Periodic Review**

- This procedure shall be reviewed annually and after any breach incident. Updates must be approved by the HMIS Committee and CoC Governance Council.

**Appendix A – Quick Incident Checklist (for staff)**

1. If you observe or suspect a breach → **Stop** any further access.
2. **Report now** to Agency Security Officer AND HMIS Lead (hmisbreach@homelesscoalition.org).
3. Secure the area/device (don't delete logs/screenshots).
4. Provide the Agency Incident Report to HMIS Lead.

**Appendix B – Agency Incident Report Form**

All agencies must complete and submit this form to HMIS Lead at **databreach@homelesscoalition.org** immediately.

Reporter Name: _____
Reporting Agency: _____
Reporter Title: _____
Reporter Phone: _____
Reporter Email: _____

Date/Time Incident Discovered: _____
Who discovered the incident: _____

Brief Description of Incident:

| |
|---|
| |

Systems/Devices Implicated:

- HMIS Web Portal
- Local Desktop
- Paper Form
- USB
- Email
- Other: _____

Known or suspected data elements exposed in breach/incident:

- Names
- Social Security Numbers
- Dates of Birth
- Personal Health Information
- Other: _____

Estimated number of affected records/individuals: _____

Actions taken to contain breach/incident thus far:

- Disabled HMIS Accounts
- Isolated Impacted Devices
- Reported to Agency Leadership
- Other: _____

Has Law Enforcement been contacted? ___ Yes ___ No
If "Yes":
Officer Name: _____
Officer Contact Information: _____