HMIS Privacy and Security Standards

As described in the 2004 HMIS Data and Technical Standards published by HUD

Last Revised: 2026

Table of Contents

Introduction

- Source and Scope of the HMIS Privacy and Security Standards
- Importance of Privacy and Security

Data Collection Limitations

- Collection of Only Appropriate and Necessary Data
- Protected Personal Information (PPI)
- Universal Data Elements (UDEs)
- Program Specific Data Elements (PSDEs)
- Local Data Elements and Organization-Specific Tools

HMIS Access and Data Sharing

- Who Can View Information in HMIS
- HMIS Acknowledgment and Release of Information (ROI)
- HMIS Consumer Privacy Notice
- Each CHO Must Have Their Own HMIS Privacy Policy
- Sharing HMIS Data Outside of HMIS

Security Standards

- CHO Responsibilities
- Paper Records and Copies

Disciplinary Process

Questions

Documents and Links

Acronym Guide

Introduction

Source and Scope of the HMIS Privacy and Security Standards

The regulations described in this document act as a summary of the Homeless Management Information System (HMIS) Privacy and Security Standards section of the 2004 HMIS Data and Technical Standards published

by the Department of Housing and Urban Development (HUD). This document will cover key points and takeaways but will not go into as much detail as the HUD document. While this document is informed by standards that come from HUD which governs Continuum of Care (CoC) projects and organizations that receive HUD funding, the Homeless Alliance of Western New York (HAWNY) has adopted and added to these standards. Since HAWNY is the CoC and HMIS Lead Agency, any organization and project that utilizes our HMIS, regardless of funding source, must adhere to the standards outlined below.

Adherence to these standards is required of every CoC and organization that collects, records, or in any way utilizes PII of clients experiencing homelessness for HMIS. HUD refers to these organizations as a covered homeless organization (CHO). This applies not only to the NY-508 region, but to the nation as a whole. Additionally, any relevant local or state laws must be followed. Notable New York State laws include; Disposal of Personal Records Law, Personal Privacy Protection Law, and The SHIELD Act. CHOs may choose to engage in additional privacy and security practices, but those outlined in this document are the minimum requirements. Other local, state, or federal laws may be pertinent depending what types of services the CHO provides and how the CHO is funded. Note HIPAA regulations take precedence over the HMIS Privacy and Security Standards for HIPAA covered organizations.

Importance of Privacy and Security

There is a moral and ethical obligation to maintain clients' privacy and security in addition to the federally mandated obligations. Through practicing and explaining proper privacy and security rights, procedures, and practices, we are able to provide the clients with autonomy and build a working relationship based on trust.

Data Collection Limitations

Collection of Only Appropriate and Necessary Data

Per HUD, a CHO is only permitted to collect PPI when appropriate and necessary for provision of homeless services, or when it is required by law.

Note that clients have the right to refuse to answer any of these questions. Whether or not they choose to provide a response should not impact their provision of services. A client cannot be denied services based on their response or lack thereof.

Protected Personal Information (PPI)

Protected Personal Information (PPI) is defined by HUD as:
"Any information maintained by or for a Covered Homeless Organization [CHO] about a living homeless individual that:

(1) Identifies, either directly or indirectly, a specific individual;
(2) Can be manipulated by a reasonably foreseeable method to identify a specific individual; or
(3) Can be linked with other available information to identify a specific individual."

Name, Date of Birth, and Social Security Number (SSN) are the three main data elements that are considered PPI, however, this is not an exhaustive list. Any information that could be used to identify a particular individual is considered PPI. This is important to remember when communicating about clients, especially over email. Regular emails are not secure and should not be used to communicate any PPI about a client. Instead, communicate by phone or use a secure email. HAWNY is able to send a secure email for the recipient to reply to upon request.

Note: Although Protected Personal Information (PPI) and Personally Identifiable Information (PII) do not have exact matching definitions, they are used interchangeably in HAWNY documents since they share the above characteristics.

Universal Data Elements (UDEs)

The UDEs are collected by all organizations in the NY-508 region that use HMIS. They include:
Demographics

- Race/Ethnicity
- Veteran Status
- Disability Status

Housing History

- Household Composition

- Homeless Status and History
- Prior Living Situation

Exit Information

- Client Destination

Program Specific Data Elements (PSDEs)

PSDEs are collected by most organizations in the NY-508 region that use HMIS. They include:

Demographics

- Disability Type
- Sex

Housing History

- Domestic Violence History

Resource Verification

- Monthly Income
- Non-cash Benefits
- Health Insurance

Coordinated Entry Information

- Current Living Situation
- Coordinated Entry Event
- Coordinated Entry Assessment

Additional PSDEs exist for certain project types.

Local Data Elements and Organization-Specific Tools

HMIS can be tailored to meet unique needs of local communities and organizations. The Local Data Elements are required by all CHOs who use HMIS in the NY-508 region. They include:

- Reason for Becoming Homeless
- Gender
- Zip Code of Last Permanent Address

Organization specific-tools and questions depend on the needs and services of a certain organization. Some potential examples include:

- Custom Assessments
- Measurements
- Case Plans

Any HMIS data elements that are not required for all CHOs by HUD remain subject to the overruling regulation by HUD that states that all information collected must be appropriate and necessary for the CHO's provision of

services and/or required by law. This additional information, especially if it contains PII, should be held to the same standards of security.

HMIS Access and Data Sharing

Who Can View Information in HMIS

Access to client information within HMIS occurs on varying levels:

- HAWNY Staff (HMIS Lead Agency and System Administrators)

Have access to all aspects of HMIS to support system administration, Coordinated Entry, reporting, and planning.

- HMIS Partners (from other organizations)

An HMIS Partner is any organization that utilizes our HMIS. Any HMIS user, regardless of the organization they work for can see your client's name, last four digits of social security number, date of birth without a Release of Information (ROI). This client information is able to be viewed by all HMIS users in order to avoid duplicate records in the system which can negatively impact client services, reporting, and ultimately funding. If the client consents to an ROI at a project, other HMIS Partners will be able to see that project entry along with the HUD standard data, UDEs, and PSDEs associated with the project entry.

- Employees and Volunteers (inside an organization)

Can access information on clients that were input by the project under which they are employed or serve under. If the client has an active ROI with another project, the standard data, UDEs, and PSDEs, associated with that project entry can also be seen.

- Clients (current and former)

May ask for print copies of their and their dependents' HMIS record.

The client maintains a level of choice throughout data collection for HMIS. As aforementioned, the client has a right to refuse to answer any of the questions without penalty. Additionally, the client has the right to choose whether or not their data can be shared between organizations within HMIS through the Release of Information (ROI).

HMIS Acknowledgement and Release of Information (ROI)

The HMIS Acknowledgement and Release of Information (ROI) form allows clients to choose whether or not their data can be shared across HMIS partner agencies. It is similar to the HMIS Consumer Privacy Notice in that it addresses client rights regarding their data and privacy, but the ROI specifically outlines consent for inter-agency data sharing and reviews specific questions or data that are usually asked or collected.

The ROI is meant to provide the client with an understanding of HMIS. This includes: what HMIS is and how it is used, what information is collected, who can access client information stored in HMIS, and a brief explanation of the benefit of choosing to allow inter-agency sharing. This document should allow the client to make an informed decision on their data sharing choice.

- A “yes” response allows the client’s data to be shared with other HMIS-participating agencies for coordination of services.
- A “no” response limits data visibility to only the project through which the client is receiving services. This means that only agency staff and system administrators (HAWNY staff) can view the client’s information.

Data that is part of the client record and is used to avoid duplicate record creation (Name, Date of Birth, Last Four Digits of SSN, and Veteran Status) is able to be seen by anyone with HMIS access unless the client has requested an anonymous profile or has selected “Client prefers not to answer” for any of these responses. These choices do not impact eligibility for services.

The HMIS Acknowledgement and Release of Information (ROI) form can be found on the HAWNY website.

HMIS Consumer Privacy Notice

The HMIS Consumer Privacy Notice is a document that discloses agency participation in HMIS. It describes why data is collected and how it may be used or shared to facilitate services as well as specific rights clients possess regarding provision of their personal information.
The purpose of this notice is to provide transparency so that clients can make informed decisions about the data they share. The most recent version of the notice is available on the HAWNY website.

The HMIS Consumer Privacy Notice must:

- Be displayed prominently in areas where client intake occurs so it can easily be accessed by clients
- Be available as a physical copy for clients to receive upon request
- State that it can and may be amended at any time and any amendments may be applied retroactively (a CHO must maintain permanent documentation of all privacy notice amendments)
- Be posted on the CHO's website (if the CHO has website)

Each CHO Must Have Their Own HMIS Privacy Policy

Every CHO must have their own Privacy Policy that covers HMIS and is specific to their organization and practices. This policy must adhere to the baseline requirements described throughout this document and cover any additional information regarding HMIS data collection, data quality, purpose and use limitations, access, and accountability while adhering to federal, state, and local laws.

Sharing HMIS Data Outside of HMIS

There are four main permitted circumstances for disclosure of client information from HMIS containing PII:

(1) To provide or coordinate services to an individual;
(2) for functions related to payment or reimbursement for services;
(3) to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or
(4) for creating deidentified PPI.

Note that CHOs can only share information that they collected from their own clients.

There are additional circumstances where a CHO may be permitted to share HMIS data containing PII outside of HMIS:

- Uses and disclosures required by law.
- Uses and disclosures to avert a serious threat to health or safety.
- Uses and disclosures about victims of abuse, neglect or domestic violence.
- Uses and disclosures for academic research purposes.
- Disclosures for law enforcement purposes.

Note that these disclosures are optional and not mandatory (unless required by law). The HUD Data and Technical Standards document elaborates on

what particular details about these circumstances may permit these disclosures.

Security Standards

CHO Responsibilities

Each CHO is responsible for implementing and maintaining, at minimum, the level of security described in this document for anywhere PII is stored/any device that is used to access HMIS.
Any device that is used to access HMIS and/or stores PII must have the following:

- A secure firewall
- Antivirus protection
- Password protection

Furthermore CHOs must ensure that:

- HMIS is accessed only through secured Wi-Fi. This means that the Wi-Fi must be password protected and not accessible by the general public
- Any usernames and passwords (for computer, laptop, HMIS, etc.) must not be written down, saved within a browser, or otherwise described in a place or manner by which they could be discovered by other individuals.
- Individual users must not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time
- Staff computers in public areas that use HMIS must be staffed at all times, or be logged out of when the staff is away from the computer
- Security systems are regularly monitored to ensure proper functioning
- HMIS data and/or PII that is electronically transmitted must be encrypted
- Notify HAWNY immediately of any potential security breaches

Paper Records and Copies

Paper copies of PII from HMIS must be stored in a secure location. When in use, the paper copy must be supervised at all times and returned to proper storage locations when no longer being used. Any hard copy of data from HMIS should be properly disposed of or deidentified after a maximum of

seven years since the copy had been created or edited (unless a different mandate by which the CHO must comply requires a longer period of time).

Disciplinary Process

All HMIS users are expected to comply with the procedures and expectations described in the HMIS User Agreement, Privacy and Security document, Data Quality Plan, and any applicable HMIS Agency Agreements. If a user fails to meet these expectations, HAWNY can implement the disciplinary process outlined below.

The disciplinary steps are applied on a case-by-case basis and may not always follow the order listed. For most general infractions, the following steps typically occur in this order. For more serious infractions, some steps, particularly the earlier ones, may be skipped.

1. Reminder (Phone or Email).

A member of the HMIS team will contact the user to bring attention to the issue and provide guidance on how to resolve it.

2. Written Warning.

If the issue is not resolved or keeps occurring, the user will receive a formal written warning via email. The warning will describe that failure to correct the issue may result in mandatory retraining or suspension of HMIS access, depending on the severity of the infraction and the discretion of the HMIS team.

3. Retraining.

The user will be retrained by the Training Coordinator at HAWNY, with a focus on any areas of concern.

4. Removal of HMIS access.

The user's access to HMIS will be revoked temporarily or permanently on a case-by-case basis.

HAWNY reserves the right to require any user to complete retraining at any time. Additionally, HAWNY may revoke HMIS access at its discretion in cases of significant breaches of the HMIS User Agreement.

Questions

Please contact the HMIS Team at HMIS@wnyhomeless.org with any questions regarding the HMIS Privacy and Security Standards.

Documents and Links

HAWNY Website – https://wnyhomeless.org/

- Document Library – https://wnyhomeless.org/document-library/
  - HMIS Acknowledgement and Release of Information (ROI)
  - HMIS Consumer Privacy Notice
  - Privacy and Security
- Knowledge Base – https://wnyhomeless.org/hmis-knowledge-base/
- Meet the Team – https://wnyhomeless.org/mission-and-vision/our-team/

HUD Exchange –

Acronym Guide

CHO - Covered Homeless Organization
CoC - Continuum of Care
HAWNY - Homeless Alliance of Western New York
HMIS - Homeless Management Information System
HUD - U.S. Department of Housing and Urban Development
LMS - Learning Management System
PII - Personally Identifiable Information
PPI - Personally Identifiable Information
PSDE - Program Specific Data Element
ROI - Release of Information
UDE - Universal Data Element