Homeless Management Information System

HMIS PRIVACY & SECURITY TRAINING

Updated Nov 2025

PRIVACY & SECURITY

This presentation emphasizes the importance of security when using HMIS.

- Defining Security & Privacy
- Basic Requirements
- Client Consent
- Confidentiality
- Laws and Regulations
- Data Ownership & Reports

WHAT IS SECURITY?

SECURITY

The safekeeping of clients' Personal Protected Information (PPI), which includes Protected Health Information (PHI), and Personally Identifiable Information (PII) and sensitive program information from unauthorized access, disclosure, use, or modification.

SECURITY REQUIREMENTS

*THESE RULES ALSO APPLY TO USERS WHO WORK REMOTELY OR USE PERSONAL DEVICES FOR HMIS.

Each Computer and Network Needs:

- A secure location - from clients AND unauthorized persons
- Anti-virus software
- Individual or network firewall

Policies for Safe Workstations:

- Passwords are NOT saved to browser or visible on desks
- Devices are locked when not in use
- HMIS accounts are not shared with coworkers under any circumstances
- Hard copies of client info are secured
- Prints are sent to a secure location

SECURITY REQUIREMENTS

*THESE RULES ALSO APPLY TO USERS WHO WORK REMOTELY OR USE PERSONAL DEVICES FOR HMIS.

Mobile Devices:

- Any mobile device must be protected by password, fingerprint, or facial recognition.
- When accessing HMIS, devices must be connected to a password-protected internet connection, never a public one. Hotspots and cellular data may be used if needed.
- Client information should not be saved to a personal device. Client documents can be uploaded directly to HMIS.
- Clients should be supervised if given a device using HMIS.

WHAT IS PRIVACY?

DATA PRIVACY

The ability of a person to determine for themselves when, how, and to what extent their own personal information is shared with others.

Those trusted with the access to personal information through HMIS must do their part in upholding this right.

Uses of HMIS

CASE MANAGEMENT

- Enrollments
- Assessments
- Referrals
- Case Notes
- Services

COMPLIANCE

- Legal
- Audits

REPORTS

- Data Quality
- Funding
- Research

BED UTILIZATION

- Bed Reservations
- Available Beds

HMIS is NOT intended for:

- PERSONAL GAIN
- STALKING
- BIAS OPINIONS
- CURIOSITY
- SHARING WITH OTHERS OUTSIDE OF SERVICE PROVIDERS

CLIENT CONFIDENTIALITY
THE FOCUS IS ON PEOPLE.

AGENCIES & INDIVIDUAL USERS OF HMIS ARE REQUIRED TO:

- comply with federal, state, and local confidentiality policies
- comply with limits to data collection: relevant, appropriate, and lawful
- post signage at intake or a comparable location with general reasons for information collection and reference to privacy policy

AGENCIES MAY INFER CONSENT FOR USES IN THE POSTED SIGN AND WRITTEN PRIVACY POLICY

Privacy Notice

for the Alliance to House Everyone Continuum of Care's Homeless Management Information System

The U.S. Department of Housing and Urban Development (HUD) requires that each jurisdiction that receives funding from HUD have a Homeless Management Information System (HMIS) in place. This agency participates in the San Antonio / Bexar County HMIS administered by Haven for Hope (H4H), a collaborative, electronic data-collection system that stores information about the individuals and families who access homeless and other human services in a community. The purpose of HMIS is to assist in determining your needs and to evaluate the effectiveness of services provided.

We will only collect information considered appropriate and necessary. The collection and use of all information is guided by strict standards of privacy, security, and confidentiality. HMIS-Participating agencies are required by law to maintain the privacy of your protected personal information, and to not access any information unless necessary.

Data Use and Disclosures

By requesting information and accepting services from this agency, you give consent for us to enter your information into the HMIS. Your information will only be shared with other HMIS-Participating agencies if written or verbal consent is received. We do not disclose your information to outside entities without your explicit written consent, except when required by law or by our funders, or for specific administrative or research purposes. These permitted disclosures are outlined in our HMIS Privacy Policies. You may request a copy of the Privacy Policy at any time. Policies may be amended at any time, and any changes will be applied retroactively

Participant Rights and Options

- You have the right to revoke consent to share any future information with other participating agencies at any time.
- You have the right to obtain and inspect a copy of your own (or your dependent's) personal record in HMIS, and request corrections if needed. Each agency is only able to provide records to which they have access.
- You have the right to request a list of all participating agencies who have access to HMIS.

Client Release of Information

for the San Antonio / Bexar County Continuum of Care's Homeless Information Management System

To provide you with the most effective and efficient service, we must collect relevant data for our Homeless Management Information System (HMIS). This secure and confidential database operated by trained representatives allows service providers to work together with you to make sure you are receiving the assistance you need in a timely manner. Beyond that, the HMIS allows the CoC to get an accurate count of all individuals experiencing homelessness or who are at risk of homelessness in San Antonio/Bexar County. To help us improve our current service system, coordinate services, and make plans for new services, we need to collect your personally identifiable information (PII). To better coordinate with other service providers, you have the right to consent to release your information to these other service providers.

Please review the information below and sign and date where indicated. *[Note to staff, if working with a family, please complete the back of this form as well].*

I understand and agree that this service provider will enter my information into the Homeless Management Information System (HMIS). The information I have provided is true and correct. I understand that my information may be shared among local service providers for the purpose of connecting me to services.

I understand that information about me that is in HMIS may be used by the service provider and the San Antonio / Bexar County Continuum of Care, including but not limited to, to conduct research and develop reports related to homelessness and housing programs, coordination of care, housing, service needs, income supports, education and employment, and program effectiveness. I authorize the collection of information, including PII, about the services provided to me and for this information to be included and shared with service providers in HMIS. I further understand that some of the information collected and shared may include records that are considered Protected Health Information under the Health Insurance Portability and Accountability Act (HIPAA). I understand that should I no longer want my information collected and shared, I may withdraw my consent in writing at any time by contacting: [Insert email address for Agency Security Officer]. Any information shared or collected prior to withdraw of consent cannot be revoked.

An agency representative has answered my questions about my privacy concerns. By signing this release form, I fully understand and agree to the above terms and conditions.

CLIENT NAME [PRINT]	DATE	CLIENT SIGNATURE	DATE

AUTHORIZED PERSONNEL NAME [PRINT]	DATE	AUTHORIZED SIGNATURE	DATE

LEVELS OF CLIENT CONSENT

- Inferred/Implied Consent: consent which is not expressly granted by a person, but rather implicitly granted by a person's actions
    - Per our Privacy Notice, consent to enter data is implied if a client chooses to be served by the agency (Notice must be posted clearly to be the case).
- Informed Consent: consent that requires a client to have sufficient information and understanding before making decisions about sharing their information
    - Clients must be given ample opportunity to understand where their information is going, who can access it, and what it will or can be used for.

COLLECTING CONSENT

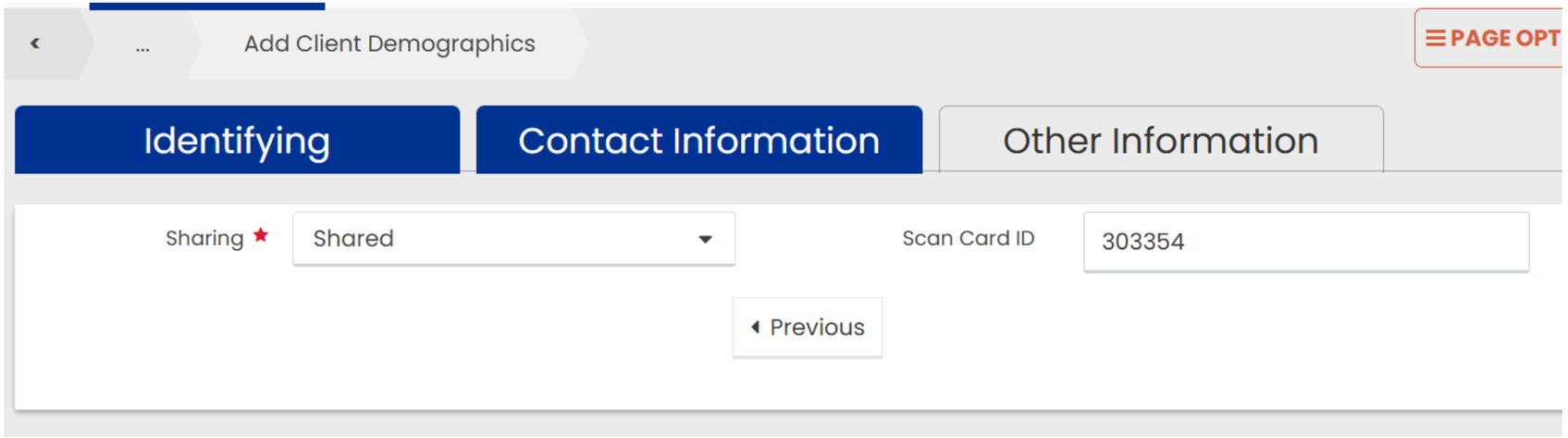
Client information cannot be shared in or out of HMIS without explicit, informed consent.

- Written Consent
  - Agencies should allow the client to review the Release of Information (ROI) and be able to explain its implications. The client can choose whether or not to consent.
  - If a client chooses to not consent, this must be noted on the ROI and in the HMIS profile. The client's profile and/or enrollment will not be shared with other agencies besides the CoC and HMIS Lead Agencies.
- Verbal Consent
  - If written consent cannot be obtained (due to client not being present or client is unable to sign) verbal consent may be given instead. Client must still be explained the implications of consent.
  - Verbal consent should still be noted on a copy of the ROI
- All proof of client consent should be retained in case proof is needed at a future date.

See section 5.5 of the Policies and Procedures

CLIENTS WITHOUT RELEASES

Clients who refuse or have not had the opportunity to sign the ROI before their profile creation must be set to Not Shared



Not Shared profiles will only be visible to the organization that “owns” the profile. They cannot be merged with other matching profiles.

PROTECTING CLIENT PRIVACY

Client information should only be searched and/or shared on a need-to-know basis.

NEED TO KNOW

- The legitimate requirement of a person to access sensitive information that is critical to the performance of an authorized, assigned mission in connection with services to a client.
- The necessity for access to specific information required to carry out official duties.
- Users must be able to support access to client's file.

PRIVACY AND SECURITY LAWS

Federal Health Insurance Portability and Accountability Act (HIPAA, 1996)

Texas Medical Records Privacy Act (MRPA, 2012)

42 CFR Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records (HHS)

HIPAA

HIPAA RULES APPLY TO COVERED ENTITIES AND BUSINESS ASSOCIATES

COVERED ENTITIES

Include certain health care providers, health plans, and health care clearing houses.

- Hospitals & Health Clinics
- Some mental health and substance abuse treatment programs

BUSINESS ASSOCIATES

Any person or entity that:

- Performs an activity or function on behalf of a covered entity that involves Protected Health Information (PHI), or
- Provides legal, accounting, management, administrative, financial, or other services for a covered entity that involves PHI

WHAT INFORMATION MUST BE PROTECTED?

You must safeguard an individual's Protected Health Information (PHI) which is collected or created as a result of providing care. These rules apply to you when you view, use, and share PHI.

PROTECTED HEALTH INFORMATION (PHI)

- Is information related to a patient's past, present, or future physical and/or mental health condition
- Can be in any form: written, spoken, or electronic
- Includes at least one of the 18 identifiers

PHI IDENTIFIERS

- Name
- Postal Address
- All elements of dates except year (ex: DOB)
- Telephone Number
- Fax Number
- Email Address
- URL Address
- IP Address
- Social Security Number
- Account Numbers
- Certificate/Licenses Number
- Medical Record Number
- Health Care Beneficiary Number
- Device Identifiers & serial numbers
- Vehicle Identifiers & serial numbers
- Biometric Identifiers (finger & voice prints)
- Full Face Photos & Other Comparable Images
- Any other unique identifying number, code, or characteristic

Potential Penalties

HIPAA & 42 CFR	Texas MRPA
Civil Penalties	
Fines up to: - "Unknowing" = $100 per violation. Annual cap of $25,000 for repeat violations - "Reasonable Cause" = $1,000 per violation. Annual cap of $100,000 for repeat violations. - "Willful Neglect but corrected w/i required time period" = $10,000 per violation. Annual cap of $250,000 for repeat violations. - "Willful Neglect not corrected" = $50,000 per violation. Annual cap of $1.5 million.	**Fines up to:** - $5,000 for each "negligent" violation in a year - $25,000 for each "knowing or intentional" violation in a year - $250,000 for each "knowing or intentional" violation in a year if PHI is used for financial gain - $1.5M if court finds a "pattern and practice", plus revocation of license and exclusion from state-funded health care programs
Criminal Penalties	
Fines and imprisonment up to: - $50,000 and 1 year in prison for "knowingly" obtaining or disclosing PHI - $100,000 and 5 years in prison if "false pretenses" - $250,000 and 10 years in prison if intent to sell PHI for personal gain or malicious harm	**N/A**
VIOLATIONS MAY ALSO RESULT IN DISCIPLINARY ACTION AGAINST YOU, INCLUDING TERMINATION	

Disclosures of PHI

PHI may be disclosed in the following instances:

WITH WRITTEN CONSENT

In accordance with client's written authorization

IF REQUIRED BY COURT ORDER

Obtain a copy of the court order

IN A MEDICAL EMERGENCY

TO REPORT ABUSE OR NEGLECT

We are required to report suspected abuse or neglect of a child, adult, or individual with disabilities; includes domestic violence

Disclosures of PHI

PHI may be disclosed in the following instances:

MISSING PERSON

MATERIAL WITNESS

VICTIM OF A CRIME

FUGITIVE

CONSULT WITH YOUR LEGAL TEAM, FOLLOW YOUR AGENCY'S POLICIES & PROCEDURES, AND INFORM THE HMIS SECURITY & COMPLIANCE SPECIALIST: ASHLEY KEOGH

Disclosures of PHI

PHI may be disclosed in the following instances:

TO THE CLIENT

With appropriate documentation

TO A LEGAL REPRESENTATIVE

Obtain a copy of the Letter of Representation and/or the Appointment Letter

FOR RESEARCH, AUDIT, OR PROGRAM EVALUATION

Must have a Research Agreement & complete the IRB process.

TO ANOTHER HEALTH CARE PROVIDER

For purposes of Treatment, Payment, or health care Operations (TPO)

All other disclosures are considered non-routine and require approval by the HMIS Security & Compliance Specialist.

DOING OUR PART

The HMIS Team monitors individual HMIS use for violations.

This includes:

- Conducting regular random audits on accounts to analyze “suspicious behavior”
- Auto-Flagging certain actions for further review
- Investigating claims/suspicions submitted by agencies, clients, or any other source
- Visiting agency locations to verify safe practices

Violations may result up to termination of HMIS access, disciplinary action, and in extreme cases, prosecution.

Remember! Everything you do in HMIS is recorded and time-stamped.

DOING YOUR PART

If you suspect that any form of Privacy or Security violation has occurred, you are obligated to report the incident to your agency's HMIS Security Officer or directly to the HMIS Security & Compliance Specialist. The HMIS Team will then conduct an investigation to verify any of the claims and provide the agency with steps on how to proceed.

Clients are also encouraged to report any concerns regarding their own HMIS profiles. Security Officers will be the first point-of-contact if a client wishes to open an investigation.

DATA OWNERSHIP

WHO OWNS THE INFO IN HMIS?

Agencies may only distribute data that they have entered or otherwise have ownership of. This includes to funders, researchers, and even clients.

REPORTING

USING HMIS TO REPORT TO FUNDERS AND OTHER ENTITIES:

- Agencies can only report on information that they themselves own.
  - Includes: Projects owned or jointly owned by the agency; Universal Data for any client that agency has served.
  - Data from other HMIS CHOs can be obtained via the Close to Home Data Request form, pending approval.
- Information should only be sent on a need-to-know basis. Only provide the minimum necessary to accomplish the goal at hand.
  - All unneeded information (especially PII) should be removed from documents as soon as possible.

REMEMBER

Use PHI only as necessary to perform your job duties

Use and disclose the minimum necessary to perform your job duties

If you need to use or disclose PHI outside of routine uses and/or disclosures, consult the HMIS Security and Compliance Specialist first.

Users are responsible for ensuring confidentiality of information even after access to HMIS has ended

Security Awareness Agreement

AGENCY/ORGANIZATION NAME: _____

LOCATION: _____

San Antonio Homeless Management Information System (HMIS)

USER CONFIDENTIALITY AGREEMENT

I understand that I will be allowed access to confidential information and/or records in order to perform my specific job duties. I further understand and agree that I am not to disclose such confidential information and/or records without the prior consent of the appropriate authority(s).

I understand that all USERID/ Passwords to access the HMIS are issued on an individual basis. I further understand that I am solely responsible for all information obtained, through system access, using my unique identification. At no time will I allow any other person to use of my USERID/Password to logon to the HMIS. I understand that accessing or releasing confidential information and/or records, or causing confidential information and/or records to be accessed or released except as allowed in the HMIS Security Awareness training, outside the scope of my assigned job duties would constitute a violation of this agreement. I understand my supervisor will be notified immediately of any violation and disciplinary action will be taken, up to termination of employment.

By affixing my signature to this document I acknowledge that I have been apprised of the relevant laws concerning access, use, maintenance and disclosure of confidential information and/or records available to me through my use of the HMIS. I further agree that it is my responsibility to assure the confidentiality of all information I access through use of HMIS, even after my access to HMIS has ended.

Pursuant to this agreement I certify that I have read and understand the laws concerning confidential information and/or records and the HMIS Security Awareness Training materials.

User Signature _____ **Date** _____ **Job Title** _____

Print User Name _____ **Email** _____

THANK YOU

Questions?

Submit a ticket to HMIS.Support@havenforhope.org