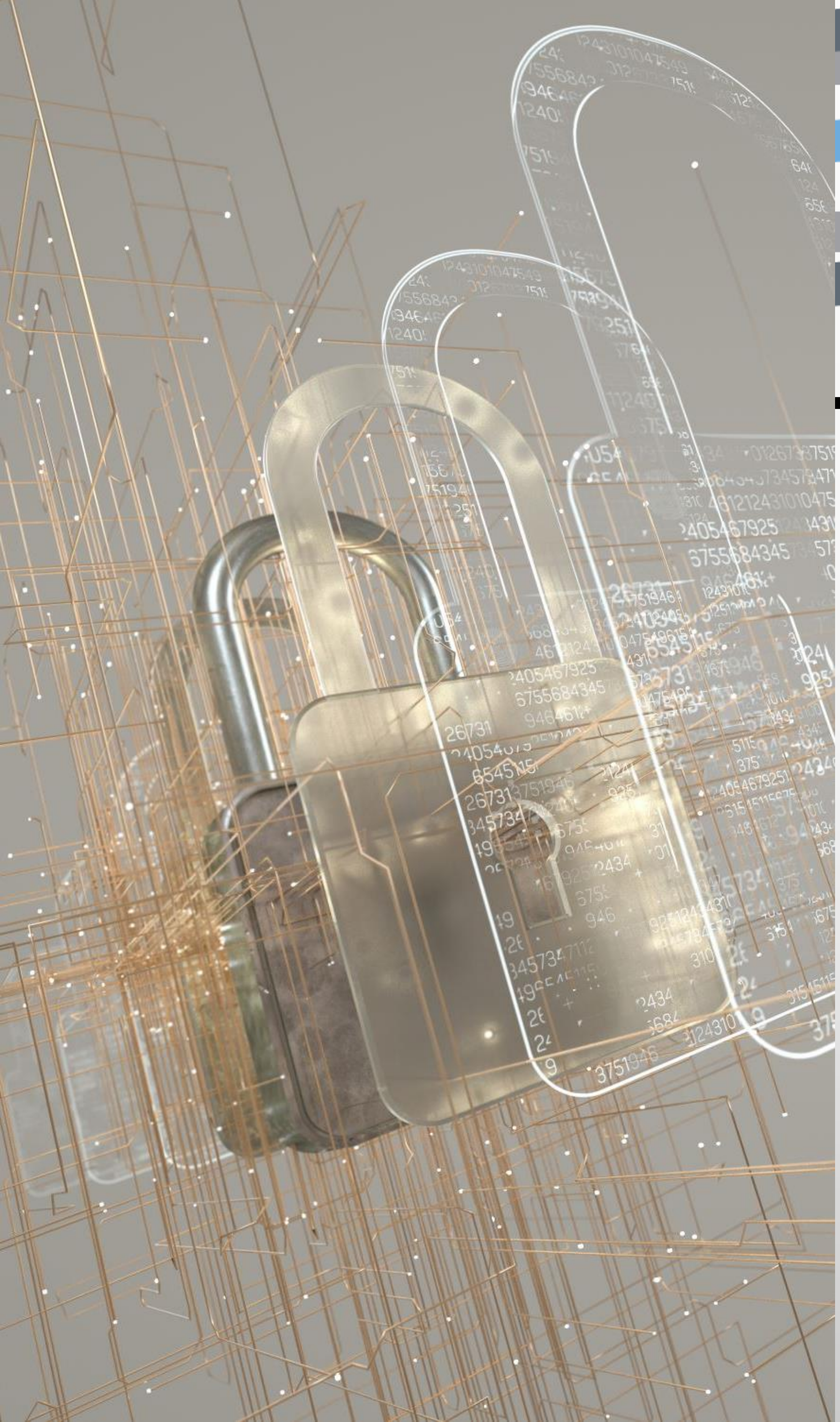
NE FL CoC
January 9, 2025

Duval | Clay | Nassau – FL 510

WELCOME
CoC Members!

HMIS Data Privacy and Security



HMIS Data Privacy and Security

- Collecting and sharing participants’ personal information is often a necessary aspect of helping resolve their housing crisis.
- It is important for providers to make informed policies and procedures and fully understand the following:
  - How data is collected, used, stored, and disclosed across system of care
  - Understand the responsibility to protect client information and be able to articulate those responsibilities to clients in a meaningful way.

HMIS Data Privacy and Security

Key Rules, Regulations, and Privacy Fundamentals

- HUD HMIS Data Technical Standards
  - Establishes standards for collecting, using, and disclosing data in HMIS
- Health Insurance Portability and Accountability Act (HIPAA)
  - Governs how health care providers, health care clearinghouses, and health plans disclose data
- 42 CFR Part 2
  - Restricts how drug and alcohol treatment programs disclose client records
- Privacy Act (5 U.S.C. 552a)
  - Requires written consent to disclose client records
- Violence Against Women Act (VAWA), Family Violence Prevention Services Act (FVPSA), and Victims of Crime Act (VOCA)
  - VAWA contains strong, legally codified confidentiality provisions that limit Victim Service Providers from sharing, disclosing, or revealing personally identifying information (PII) into shared databases like HMIS
- State and local privacy laws
  - May place additional restrictions on sharing, using, or disclosing data
  - When privacy laws conflict, use the more restrictive law and the higher standard

HMIS Data Privacy and Security

Implications for Victim Service Providers

- Domestic violence providers are prohibited from entering PII into HMIS, and must use a comparable database
  - This database must be comparable to HMIS in its capacity to support HUD privacy and security requirements and at a minimum, meet Data Standards requirements and produce HUD required reporting files.
- Victims of domestic violence must have access to the coordinated entry process
  - May be through a separate access point and assessment tool
  - Safety and confidentiality is essential when sharing data or referring clients
  - All data use and disclosure policies and procedures should be developed to ensure that regardless of where the household fleeing domestic violence presents for service, safe and equal access to homeless services and housing programs is provided while protecting their information.

HMIS Data Privacy and Security

Data Privacy Requirements

- HUD requires the CE process to adhere to the baseline HMIS privacy requirements for all methods of data collection, use and disclosure, including electronic, paper and verbal disclosures.
- At a minimum, the CoC’s privacy standards should be communicated through two primary methods:
  1. CoC’s Coordinated Entry Policies and Procedures; and
  2. Privacy Notice, which includes:
     - Description of participant rights,
     - Participant options*,
     - Provider’s responsibilities to protect PII, and
     - How the provider will use and disclose the participant’s information
- *Reminder: CoCs are prohibited from denying services to participants if they refuse their data to be shared, unless federal statute requires so as a condition of program participation (HUD Coordinated Entry Notice: Sections II.B.12.c and II.B.13)

HMIS Data Privacy and Security

Data Privacy Requirements

- A provider must collect PII by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.
- When required by law to collect information, providers are not required to seek participant consent
  - In these required instances, participants may refuse to provide the information and still receive services, but the provider must ask
- In all circumstances, providers should make data collection transparent by providing participants with a written copy of the privacy notice

HMIS Data Privacy and Security

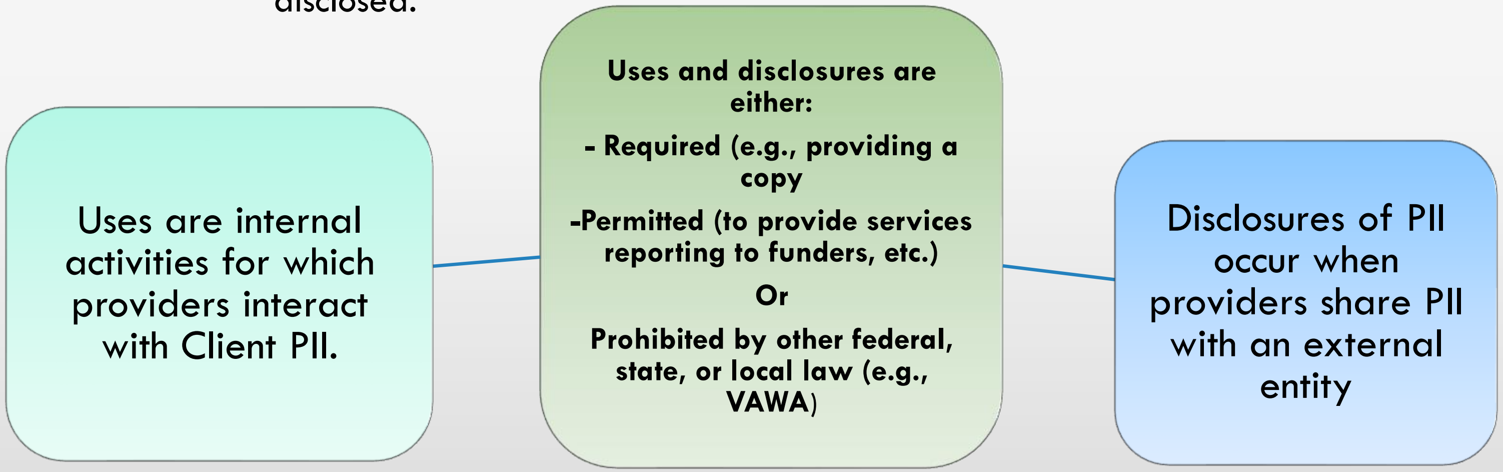
Public Statement Example

“ We collect personal information directly from you for reasons that are discussed in our privacy notice. We may be required to collect some personal information by law or by organizations that gives us money to operate this program. The personal information we collect is important to run our programs, to improve services for persons experiencing homelessness, and to better understand the needs of persons experiencing homelessness…”

HMIS Data Privacy and Security

DATA USES AND DISCLOSURES

Once data is collected, providers have obligations about how that information is used and disclosed.



Uses are internal activities for which providers interact with Client PII.

Uses and disclosures are either:

- Required (e.g., providing a copy

-Permitted (to provide services reporting to funders, etc.)

Or

Prohibited by other federal, state, or local law (e.g., VAWA)

Disclosures of PII occur when providers share PII with an external entity

The provider's uses (internal) and disclosures (external) of collected information must be stated in the privacy notice.

HMIS Data Privacy and Security

DATA USES AND DISCLOSURES

- PROVIDING OR COORDINATING SERVICES TO AN INDIVIDUAL
- CREATING DE-IDENTIFIED CLIENT RECORDS FROM PII
- CARRYING OUT ADMINISTRATIVE FUNCTIONS (E.G., LEGAL, AUDIT, PERSONNEL, OVERSIGHT, AND MANAGEMENT FUNCTIONS)
- FUNCTIONS RELATED TO PAYMENT OR REIMBURSEMENT FOR SERVICES

HMIS Data Privacy and Security

DATA USES AND DISCLOSURES

Providers are also allowed (in some cases required) to disclose information in the following ways without participant consent, as long as they are clearly documented in the privacy notice.

- 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 research purposes
- Uses and disclosures for law enforcement purposes

Important: Uses and disclosures not listed in the privacy notice require the participant’s consent

HMIS Data Privacy and Security

AUTHORITY TO DISCLOSE IS NOT UNLIMITED

If a legal entity or public health agency is not seeking or requiring individual ppi, then ppi should not be disclosed

If it is sufficient to give adequate information to a provider without disclosing ppi of one or more participants, then it would be appropriate not to disclose ppi.

Do not send a list of all participants to a provider if only one individual is being referred or a subset of individuals are being referred

HMIS Data Privacy and Security

Uses and Disclosures that require consent

Authorization Forms are required for both uses and disclosures of PII that are not required or permitted per HUD’s 2004 HMIS Data and Technical Standards. This should occur if the CoC identifies uses or disclosures that are necessary to make the CE process operate effectively and efficiently, yet those uses and disclosures are not permitted without consent per HUD’s 2004 HMIS Data and Technical Standards.

Many CoCs currently use a form called a “release of information” (ROI).

- ROIS are commonly used to gain consent for disclosures but they might not include uses.
- If your CoC uses an ROI, be sure that it indicates both data disclosures and data uses for which consent is required

HMIS Data Privacy and Security

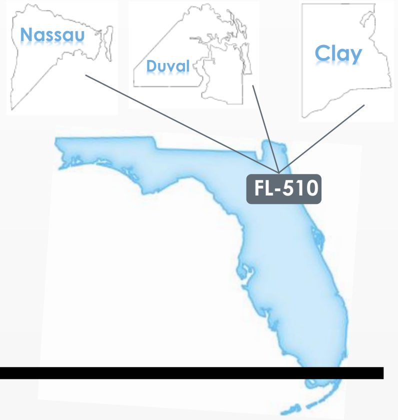
DATA SECURITY

Data Security

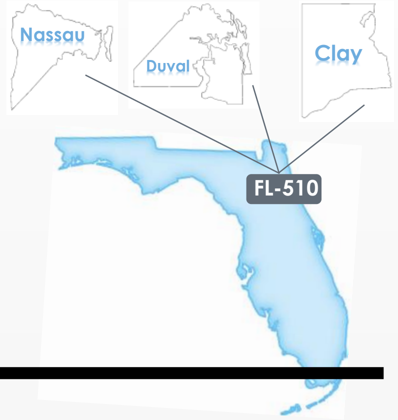
- ClientTrack is in constant communication with the HUD office and meets all the standards and requirements for data security.
- HMIS team sends out a security check-list to new agencies at the time of project set-up

Physical Workstation Security

- Access to workstations must be controlled and monitored
  - If not continuously staffed must be secured
- Workstation requires username and password
- Password protected locking screen saver
- Stored in a secure location- locked office area



HMIS User Agreement



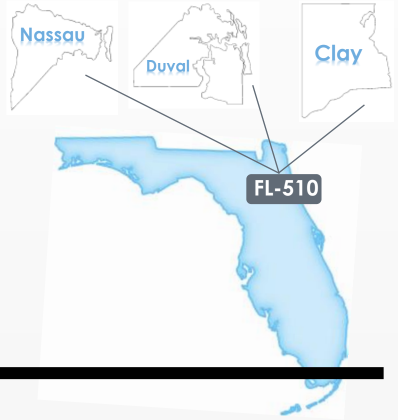
2025 Point-In-Time Count

Point-In-Time Count – January 30th

Sheltered Count Planning Meeting | January 9th at 1 pm.

Join Zoom Meeting
https://us02web.zoom.us/j/86098944145?pwd=IAY9RpZ6GsrdWt90wsLMTbeArC5xSb.1

Meeting ID: 860 9894 4145
Passcode: 311919



Events & Announcements

What’s new with YOU?

Questions?

Thank you!