WELCOME
CoC Members!
Collaborative Applicant Update

2021 Point In Time Count
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 Annual Training

**HMIS Data privacy and security**

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

---

**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…”
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.

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

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)

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

HUD gives providers the authority for the following uses and disclosures without needing to obtain participant consent as long as they are clearly articulated in the Privacy Notice.

- 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
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.
Types of Uses and Disclosures

Mandatory:
• Client access to their information; and
• Disclosures for oversight of compliance with HMIS privacy and security standards.

Permitted:
• To provide or coordinate services to an individual
• For functions related to payment or reimbursement for services
• To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; and
• For creating de-identified from PII
Types of Uses and Disclosures

**Additional permissions:**
- 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; and
- Uses and disclosures for law enforcement purposes

**Important Information**
- You must have a sign indicating that you collect data and enter it into HMIS (or a comparable database if required)
- Participants may refuse to give PII and still receive services

*Best practice is to provide a copy of the Privacy Notice and verbally explain it in plain language to all participants*
Specific CE activities can be enhanced if PII is disclosed among CE providers—these are covered under the permitted use and disclosure: *to provide or coordinate services to an individual*. Below are some examples that the CoC may wish to include for purposes of transparency and clarity:

**Use and disclosure for coordinating care.** Disclosing information to multiple CE providers that are assisting to connect the individuals to appropriate resources and services.

**Use and disclosure to determining client prioritization for housing.** Disclosing assessment data can help staff determine the placement of an individual on a prioritization list and if needed develop a safe sheltering plan while the individual is waiting for placement into permanent housing.

**Use and disclosure for making referrals.** Disclosing client information can help match a person to the right resource and potentially create multiple referral options.

**Use and disclosure for determining participant progress.** HMIS can be used to build a single participant record that contains information through the CE process from access to project enrollment.
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.

**Privacy and Security Grievances:** CHOs are responsible for the following—

Establishing procedures for accepting and considering questions or complaints about its privacy and security policies and practices.

Requiring each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.
Data Security

• ClientTrack is in constant communication with the HUD office and meets all the standards and requirements for data security.

• HMIS teams 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 username and password
• Password protected locking screen saver
• Stored in a secure location- locked office area
CoC Governance Board Update
Events & Announcements

News YOU can use
Micah's Place

Holiday Gift Card Drive

Now - December 16th
Events & Announcements

City Rescue Mission

Shoeboxes of Love

Now - December 18th
Events & Announcements

City Rescue Mission

Christmas Meal

Tuesday, December 22nd

[Image of Christmas Meal announcement]
Thank you!

Dawn Gillman, CEO
904.354.1100 | dgilman@changinghomelessness.org