

Domestic Violence Data Collection Protocols

**Prepared by the Ohio Domestic Violence Homeless
Management Information System Workgroup**

Table of Contents

Table of Contents	2
Introduction	3
Background.....	3
Definitions	3
Comparable Database	3
Domestic Violence	4
Homeless Management Information System (HMIS)	4
Personally Identifying Information (PII).....	4
Victim Service Provider (VSP)	4
Informed Consent	4
Three Components of Consent.....	5
Allowable Uses and Disclosures	5
Consent Protocols.....	5
Interviewing.....	5
Interviewing Protocols	5
Data Storage.....	6
Data Storage Protocols	6
Data Transfer	6
Data Transfer Protocols	6
Statutory Guidance	6
HUD HMIS Rule	6
CoC Rule.....	6
Equal Access Rule	6
Fair Housing Act.....	6
Violence Against Women Act (VAWA).....	6

Introduction

In 2018, the Coalition on Homelessness and Housing in Ohio (COHHIO) invited Ohio Domestic Violence Network (ODVN) and each Housing and Urban Development (HUD) Continuum of Care (CoC) in the state of Ohio to participate in a workgroup looking specifically at the intersection of Homeless Management Information Systems (HMIS) and services for survivors. This group continues to meet on average quarterly. For more information email hmis@cohhio.org. Topics covered by this workgroup have included complying with HUD's comparable database requirement, trauma-informed assessment options, and best practices around data collection, storage and transfer. This document is a summary of those best practices around data and is intended as a resource for HMIS Administrators, Victims Service Providers (VSPs) and homeless service providers.

Background

The experiences of homelessness and domestic violence often intersect. Domestic violence threatens a victim's housing because the home may be the primary site of the abuse. Housing instability can make it difficult to escape a domestic violence situation, particularly when children and pets are involved. Unfortunately the service streams designed to address homelessness and domestic violence have developed independently of one another and historically have not sufficiently informed one another's efforts. Now HUD and the Office on Violence against Women (OVW) are working to bridge that gap, and leaders in Ohio are committed to continuing that work at the state and local levels.

HUD requires all CoC funded programs to enter client level data in to a Homeless Management Information System (HMIS). HUD publishes parameters for this database but does not provide nor endorse a specific product. As a result, HMIS implementations vary based on product used as well as local organization. HMIS data is used to describe a CoC's homeless population, both in demographics and services received. The purpose of this data collection is to understand more about populations experiencing homelessness and evaluate the success of programs in ending homelessness. Requirements around privacy and security are included in HUD's HMIS specifications.

OVW discourages client level data collection because of the security concerns specific to survivors of domestic violence. When a victim leaves, it is the most dangerous time for them as their abuser reacts poorly to the perceived loss of control over the victim. Should the abuser find out where the client is located directly or indirectly from data collection it could be dangerous for the client. As a result, OVW stipulates that any required reporting on service provision must always be in the aggregate. This restriction also applies to funding from the Family Violence Prevention and Services Act (FVPSA) and the Office for Victims of Crime (OVC). Projects funded through these streams are prohibited from entering any data into HMIS. If the projects are also funded by HUD, they are required to use a comparable database.

Once a client leaves an OVW, FVPSA or OVC funded project, legally those data protections no longer apply to the client. If the client goes on to a wholly HUD funded project, only the HMIS requirements around privacy and confidentiality apply. As a result, some VSPs are reluctant to refer clients to HUD funded projects because they do not trust that the survivor's data will be adequately secured in HMIS. In an effort to build trust, these protocols outline recommendations to protect survivor data in HMIS.

Definitions

Comparable Database

A comparable database must be a relational database that meets all HMIS data standards and the minimum standards of HMIS privacy and security requirements. It also must be able to produce the .csv files required by HUD (HMIS Comparable Database Decision Tree).

Domestic Violence

Domestic Violence includes felony or misdemeanor crimes of violence committed by a current or former spouse of the victim, by a person with whom the victim shares a child in common, by a person who is cohabitating with or has cohabited with the victim as a spouse, by a person similarly situated to a spouse of the victim under the domestic or family violence laws of the jurisdiction receiving grant monies, or by any other person against an adult or youth victim who is protected from that person's acts under the domestic or family violence laws of the jurisdiction (VAWA).

Homeless Management Information System (HMIS)

A Homeless Management Information System is the information system designated by a local Continuum of Care (CoC) to comply with the requirements of CoC Program interim rule 24 CFR 578. It is a locally administered data system used to record and analyze client, service, and housing data for individuals and families who are homeless or at risk of homelessness (HMIS Data Standards).

Personally Identifying Information (PII)

Personally Identifying Information means individually identifying information for or about an individual including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, regardless of whether the information is encoded, encrypted, hashed, or otherwise protected, including a first and last name; a home or other physical address; contact information (including a postal, email or Internet protocol address, or telephone or facsimile number); a social security number, driver license number, passport number, or student identification number; and any other information, including date of birth, racial or ethnic background, or religious affiliation, that would serve to identify any individual (VAWA). The National Network to End Domestic Violence considers all client level data to be personally identifying.

Victim Service Provider (VSP)

A victim service provider is a private nonprofit organization whose primary mission is to provide direct services to victims of domestic violence. This term includes permanent housing providers-including rapid re-housing, domestic violence programs (shelters and non-residential), domestic violence transitional housing programs, dual domestic violence and sexual assault programs, and related advocacy and supportive services programs (HUD).

Informed Consent

Informed consent refers to a client's agreement to receive services based on a complete understanding of the potential benefits and risks associated with those services. Informed consent is a critical component of ethical service, but is complicated by the experience of trauma. There is a potential that a client in a domestic violence and/or housing crisis will sign anything that is handed to them in an effort to get help without fully understanding the document. In an effort to mitigate this possibility, it is incumbent upon the housing worker to provide the best information possible to assist a client in understanding their rights, including the data that will be collected about them and how it will be used.

For domestic violence survivors, informed consent is particularly important around the coordinated entry process. The nine Continua of Care in Ohio each have their own coordinated entry process, which may or may not include victim service providers as access points to the homeless system. When referring to or from a victim service provider it is important to be clear that HUD prohibits victim service providers from entering in to HMIS and that they instead must use a comparable database to collect non-personally identifying information.

Homeless coordinated entry service providers that use HMIS should only share a survivor's information with the full, verbal or written consent of that survivor. In addition to explaining the benefits of participating in the coordinated entry prioritization assessment, it should also be fully explained to the survivor that any client may

decline to participate in a prioritization assessment without being penalized or losing the opportunity to be placed on the prioritization list for available housing per the CoC's policies. To learn more about serving domestic violence survivors in the coordinated entry process [click here](#).

Three Components of Consent

Informed consent includes three key components:

1. **Privacy Posting:** HUD requires a privacy posting be visible in any area where data is collected for HMIS.
2. **Acknowledgment of Data Collection:** According to HUD, acknowledgment of data collection can be inferred by the presence of the privacy posting. Each CoC must decide if they will accept inferred consent or require explicit consent for data collection.
3. **Consent to Share:** To share a client's data with other providers, such as in an HMIS where data is visible between providers, time limited consent should be obtained from the client.

Allowable Uses and Disclosures

The 2004 HMIS rule outlines several allowable uses and disclosures of PII including:

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
4. For creating de-identified PII

Additional uses and disclosures are "permissive and not mandatory." CoCs should be mindful of how their HMIS Policies and Procedures outline allowable uses and disclosures and make sure that they are as restrictive as possible. To provide or coordinate services to an individual includes the process of permanent housing (PH) prioritization as required under Coordinated Entry (CE). Housing providers are responsible to ensure that all participants in the prioritization process agree to abide by the housing provider's Policies and Procedures regarding privacy and confidentiality. Only the minimum amount of data necessary for an appropriate housing referral (outlined below under Data Transfer) should be shared in the prioritization meetings.

Consent Protocols

1. Written consent forms should be double locked (in a locked filing cabinet in a locked room) or uploaded to a local computer and locked.
2. Specific data items to be collected and agencies who have access to the data should be listed in a written consent form. The list should be updated no more than annually.
3. Depending on the level of consent given by the client, each CoC has to determine whether or not they use anonymous data entry, lock records, or both.

Interviewing

The intake interview is an important opportunity to discover if a client is experiencing domestic violence. There are a variety of things a housing worker can do to improve the likelihood that a client will disclose their experience. Disclosure allows the worker to provide support and appropriate referral to the client.

Interviewing Protocols

1. Interview adults separately.

2. Interview clients in an area as private as possible.
3. Develop training for staff on trauma-informed interviewing.
4. Conduct safety planning and threat assessment.

Data Storage

Once data is collected from a client, particularly PII, the housing worker has to store that data responsibly.

Data Storage Protocols

1. No VSP data should ever be stored in HMIS.
2. Paper forms should be double locked and/or shredded after use.
3. Electronic documents should be password protected on a password protected machine.

Data Transfer

Only the minimum amount of survivor data should be transferred for the purposes of referral.

Data Transfer Protocols

1. No PII should ever be transmitted electronically.
2. Name and contact information should only be shared in-person, by phone or non-electronic fax.
3. The following information can be transmitted electronically with a personal identifier that is only shared in-person or over the phone;
 - a. Provider referring
 - b. Size of unit needed
 - c. Area where client wants to live
 - d. Any imminent safety concerns

Statutory Guidance

[HUD HMIS Rule](#)

Document from 2004 that outlines the basic privacy and security requirements for an HMIS

[CoC Rule](#)

Outlines the requirements for CoC Programs

[Equal Access Rule](#)

Outlines requirement that HUD's housing programs be open to all eligible individuals and families regardless of sexual orientation, gender identity, or marital status

[Fair Housing Act](#)

Includes protections for survivors of domestic violence

[Violence Against Women Act \(VAWA\)](#)

Funds services for survivors of domestic violence