Overview

The Continuum of Care Interim Regulation (24 CFR Part 578.7) describes that the Continuum of Care is responsible for reviewing, revising, and approving a **privacy plan, security plan, and data quality plan** for the HMIS. On July 30, 2004, the US Department of Housing and Urban Development (HUD) released the privacy and security standards for Homeless Management Information Systems (69 Federal Register 45888). This Privacy Plan is intended to be consistent with the HUD standards. All users, agencies and system administrators must adhere to this Privacy Plan.

We intend our Privacy Plan to support our goal of providing an effective and usable case management tool. We recognize that clients served by individual agencies are not exclusively that "agency's client" but instead are a client of the Maricopa County Continuum of Care. Thus, we have adopted a Privacy Plan which supports an open system of client-level data sharing amongst agencies whenever a client consents to do so.

The core tenant of our Privacy Plan is the Baseline Privacy Notice. The Baseline Privacy Notice describes how client information may be used and disclosed and how clients can get access to their information. Each agency must either adopt the Baseline Privacy Notice or develop a Privacy Notice which meets and exceeds all minimum requirements set forth in the Baseline Privacy Notice (this is described in the Agency Responsibilities section of this Privacy Plan). This ensures that all agencies who participate in the HMIS are governed by the same minimum standards of client privacy protection.

Although the Baseline Privacy Notice and its related forms are appendices to this Privacy Plan, they act as the cornerstone of our Privacy Plan.

All amendments to the Privacy Plan (including changes to the Baseline Privacy Notice and related forms) are approved by the Continuum of Care Board.

Privacy Plan Document/Form	Description	Use
Baseline Privacy Notice	This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency collects, utilizes and discloses information.	Agencies must adopt a privacy notice which meets all minimum standards.
Maricopa Regional Continuum of Care Data Sharing ROI	This form notifies clients about the Privacy Notice and obtains their consent to share data within the HMIS.	Agencies must present an approved ROI to every client they serve that will be entered into HMIS.
List of Current Universal Data Elements & Participating Agencies	This outlines the list of shared data elements and agencies to whom those data elements are shared.	Agencies must be able to direct clients to this document.

Global Data Sharing

Data sharing of the HUD Universal Data Elements among participating HMIS agencies began in 2013. Agencies participating in HMIS are expected to request client consent to share the HUD Universal Data Elements. In April of 2020, the Continuum agreed to expand the Universal Data Element fields that are shared with all providers. These fields include basic client demographic information, questions to determine chronicity, income, non-cash benefits, disabilities, health insurance and client notes that are designated to be shared system-wide. Agencies which are prohibited from participating in data sharing (ex HOPWA, some RHY Programs) are exempt from this requirement. Agencies who have a legal justification for not requesting client consent to share the HUD Universal Data Elements may request an exemption from the Data Sub-Committee.

Participating Agencies that are HIPPA covered entities, must adhere to the privacy and informed consent procedures as outlined in their internal processes and procedures. Further, these agencies have the responsibility of communicating with the HMIS Lead what data should not be shared per their requirements.

Affinity Group Data Sharing

Some agencies may need to share data based on a business need-to-know and coordination of care for particular sub-populations of individuals and families experiencing homelessness. These sharing groups are called "Affinity Groups." This type of data sharing is in addition to the HUD Universal Data Element system-wide sharing.

The HMIS Lead has the discretion to approve or limit the number of affinity groups. Agencies wishing to form an affinity group must develop a data sharing Memorandum of Understanding (MOU) and provide that to the HMIS Lead. The MOU must include:

a. The agencies that agree to share data
b. A list of data elements that will be shared in addition to the standard Global sharing
c. The programs at each agency that will be entering the data. (Agreement must note that data will be shared to the entire agency but that only certain programs may enter the data.)
d. A description of the consent process. What, if any, additional consent will be required from the client.
e. Identification of the key point people at each agency
f. Signatures from executive leaders

Verbal ROI

The collection of a client's consent via verbal ROI is permitted at the discretion of the Data Sub-committee. Request for permission to use a Verbal ROI will be considered when:

a. There's a specified community or agency need, AND
b. The agency has a method to document the ROI, AND
c. The agency provides a verbal ROI script for the Data Sub-Committee to approve. (It is suggested that the verbal ROI follow the standard ROI template available from the HMIS Lead)

A verbal ROI will be approved on a per-program basis. Generally, an entire agency would not be permitted to collect a verbal ROI, as this accommodation should only be allowed for programs when necessary.

Domestic Violence
The Violence Against Women Act (VAWA) and the Family Violence Prevention and Services Act (FVPSA) contain strong confidentiality provisions that limit the sharing of victims' personally identifying information, including entering information into public records and databases.

These provisions affirm confidentiality practices that protect the safety and privacy of victims of domestic violence, dating violence, sexual assault, and stalking. HMIS systems must protect the confidentiality of victims of domestic violence, dating violence, sexual assault and stalking seeking housing assistance. It requires that **both the HMIS and agencies** reasonably protect the identity of victims by refraining from disclosing personally identifying information.

Agencies and programs designed specifically to provide services to victims of domestic violence, dating violence, sexual assault and stalking are **prohibited** from entering **any information** into HMIS.

Agencies that have a domestic violence program, but are not designated as a domestic violence agency must complete the DV Self Certification form to demonstrate to the HMIS Lead and the Data Sub Committee that they are eligible to enter information into HMIS. If an agency wishes to enter anonymous/de-identified information into HMIS, this must be approved by the Data Sub Committee due to the data quality concerns and lack of coordination that will result.

User Responsibilities
A client's privacy is upheld only to the extent that the users and direct service providers protect and maintain their privacy. The role and responsibilities of the user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client or their data. (This could potentially be any person at the agency: a staff member, volunteer, contractor, etc.)

Users have the responsibility to:

- Understand their agency's Privacy Notice and ROI
- Be able to explain their agency's Privacy Notice and ROI to clients
- Follow their agency's Privacy Notice
- Know where to refer the client if they cannot answer the client's questions
- Present the Privacy Notice and ROI to the client before collecting any information
- Uphold the client's privacy in the HMIS

Agency Responsibilities
The 2004 HUD HMIS Standards emphasize that it is the agency's responsibility for upholding client privacy. All agencies must take this task seriously and take time to understand the legal, ethical and regulatory responsibilities. This Privacy Plan and the Baseline Privacy Notice provide guidance on the minimum standards by which agencies must operate if they wish to participate in the HMIS. Meeting the minimum standards in this Privacy Plan and the Baseline Privacy Notice are required for participation in the HMIS. Any agency may exceed the minimum standards

described and are encouraged to do so. Agencies must have an adopted Privacy Notice which meets the minimum standards before data entry into the HMIS can occur.

Agencies have the responsibility to:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in this Privacy Plan and Baseline Privacy Notice (examples: Substance Abuse Providers covered by 24 CFR Part 2, HIPPA Covered Agencies, Legal Service Providers).
- Review the 2004 HUD HMIS Privacy Standards (69 Federal Register 45888)
- Adopt and uphold a Privacy Notice which meets or exceeds all minimum standards in the Baseline Privacy Notice as well as all industry privacy standards. The adoption process is to be directed by the individual agency. Modifications to the Baseline Privacy Notice must be approved by the Data Sub Committee.
- Ensure that all clients are aware of the adopted Privacy Notice and have access to it. If the agency has a website, the agency must publish the Privacy Notice on their website.
- Make reasonable accommodations for persons with disabilities, language barriers or education barriers.
- Ensure that anyone working with clients covered by the Privacy Notice can meet the User Responsibilities.
- Designate at least one user that has been trained to technologically uphold the agency's adopted Privacy Notice.

System Administration Responsibilities (HMIS Staff)

HMIS Staff have the responsibility to:

- Adopt and uphold a Privacy Notice which meets or exceeds all minimum standards in the Baseline Privacy Notice.
- Train and monitor all users on upholding system privacy.
- Monitor agencies to ensure adherence to their adopted Privacy Notice.
- Develop action and compliance plans for agencies that do not have adequate Privacy Notices.
- Maintain the HMIS Website to keep all references within the Baseline Privacy Notice up to date.
- Provide training to agencies and users on this Privacy Plan.