HMIS Data Sharing MEMO: Sharing Client Information

This memo provides general guidance on recent updates to HMIS policies & procedures made in November 2025, including the shift to verbal client consent. This memo is intended for Multnomah County partners and programs utilizing HMIS.

These updates clarify data sharing policies, enabling easier care coordination and service navigation.

Goal of this Memo

- Answer frequently asked questions about sharing client information.
- Empower providers to confidently share information both with each other and with cross-sector partners.
- Clearly define what can be shared for care coordination.
- Support providers in helping clients access all of the services they want, need, and are entitled to - meeting the needs of the whole person.

What is Care Coordination & Navigation?

If you answer "Yes" to any of the following, you are performing a vital role in our system:

Connecting & Accessing: Do you help clients find and use essential services like housing, food programs, healthcare, or disability support?

Removing Barriers: Do you assist with practical "heavy lifting," such as completing paperwork and managing schedules, so clients can maintain their care?

Bridging the Gap: Do you ensure that services from different providers are well-organized and working together toward a single goal?

******* This is care coordination & navigation! *******

Care coordination & navigation allows us to share info in order to:

- Allow collaboration between service providers for the benefit of their shared client
- Coordinate new services that haven't been established yet
- Enable warm hand offs between providers
- Explore other potential services

What Information Can Be Shared?

For the purposes of care coordination & navigation, **organizations / roles that do not provide healthcare (i.e. non-HIPAA covered entities)** can share relevant personal identifiable information (PII), healthcare, disability, and social needs information.
It is allowable to share:

- self-disclosed substance use disorder (SUD) information,

- self-disclosed health information and/or
- domestic violence information

...if the information is sourced from HMIS or collected by non-healthcare, non-victim service providers. However, doing so should be done with discretion and only when necessary.

Be advised that some agencies that provide housing and also provide healthcare or victim services are covered by HIPAA, 42 CFR Part 2 and/or VAWA and require a release of information in order to coordinate care.

Examples of Personal Identifiable Information (PII) *(including but not limited to)*

- First and Last Name
- Date of Birth
- Social Security Number
- Race & Ethnicity
- Gender
- HMIS Program Information

Examples of Health, Disability and Social Needs *(including but not limited to)*

- **Self Disclosed Health Information:** *Diagnosis, Conditions, Needs, etc.*
- **Disability Information:** *Physical Limitations, Use of or Need for Medical Equipment, Activities of Daily Living (bathing, toileting, dressing) etc.*
- **Social Determinants of Health:** *Income, Food, Transportation, Education Needs etc,*
- **Health Plan Coverage**: *Plan Assignment, PCP Clinic etc.*

What NOT to Share!

Only share what is vital to the client's care: Limit information to the minimum necessary for successful service navigation and coordination.

If your agency is covered by HIPAA, NEVER SHARE: HIV status or other health-related information ***without a specific, time-limited, written release of information.*** See FAQ below for more information.

If your agency is covered by 42 CFR Part 2, NEVER SHARE: SUD treatment records ***without a specific, time-limited, written release of information.***

Victim services providers, covered by VAWA, enter information into a different system than HMIS.

Data sharing should never be used in a way that causes harm to clients

(including but not limited to)

- Stigma, Discrimination, Reinforcing Biases
- Immigration, Criminal, and Legal Risks
- Targeting of Vulnerable Locations or Displacement
- Exploitation
- Erosion of Trust
- Forced Treatment
- Exposure of Domestic Violence Survivors
- Identity Theft

Who Can Share & Receive Information?

HMIS Users & HSD Program Staff can share and receive information with each other and external partners.

Different Types of Consent

There are three sets of policies that people can use to share HMIS information depending on the situation.

Although not all information is entered directly into HMIS, all data collected by HMIS users is relevant for client care coordination and navigation purposes.

1. **HMIS Privacy and Security Notice -** an overarching set of policies that governs all HMIS data
   The current notice as of this writing was revised in November 2025 and applies to all information in HMIS. It allows:
   - Use and sharing of client information to **"plan, provide, coordinate and improve services"**
   - **Ability to locate other programs and services** that may be able to assist clients
   - **Administrative activities** (including legal, audit, program evaluation, planning, analysis, reporting, oversight, or management)

Note: The Privacy & Security Notice - and not this document - drives policy. In the event that policy changes over time, consult the latest Privacy & Security Notice directly.

Take Away: Sharing HMIS information without consent is **ALLOWED, BUT** should be limited until informed consent is obtained. Share info for intermittent navigation and connection to care or services, only as needed.

2. **Verbal Consent -** Determines consent for data sharing within HMIS. Used in conjunction with the Privacy and Security Notice. The HMIS Verbal Release of Information (ROI) form is completed every time a client is assessed or enrolled in services that are entered into HMIS. Information from the verbal consent form is transacted in HMIS following collection. This process:

- Indicates whether the participant agrees to share their collected data with other agencies within HMIS
- Allows for client's services to be shared and viewed in HMIS by other providers for continuity of service and care coordination
- **Non-Consent to the HMIS Verbal ROI does not limit coordination of care** - *see Privacy and Security Notice section above*

Take Away: Verbal consent to share HMIS data allows HMIS Users to view and share clients' program enrollment information within HMIS. This facilitates care coordination and continuity of care.

3. **Written Release of Information**
   A formal, written document that allows for the sharing of an individual's confidential personal and health information, which explains the purpose of sharing information, who it is shared with, how the information can be used and is time limited.

When and why is it required?
Although the Homeless Services Department (HSD) doesn't require a written release for providers and staff to coordinate care, getting a signed release is still considered a best practice. A written ROI, helps ensure staff understand the client's wishes and that clients understand what support staff will provide to them.
- AND -
While HIPAA allows care coordination between organizations that provide healthcare **(i.e HIPAA-covered)** and those that do not **(i.e non-covered, meaning that HIPAA does not regulate disclosure of information)**, without needing client permission, many HIPAA-covered organizations still require a signed release of information form to disclose information and engage in coordination.

Certain situations are protected by stricter regulations, including:

- DV Status / Information
- Substance Use Disorder Diagnosis / Treatment Records
- HIV Status
- Ongoing Data Sharing
- When sharing data with organizations that provide healthcare

Data Sharing Best Practices

- Ensure services are client driven and person-centered.
- Limit data shared to minimum information necessary.
- Obtain authorization to share data as soon as possible and ensure the client understands what and why information is being shared.

- Information must be shared in a manner that respects the privacy and security of clients.
    - Verbal communication - Information should not be shared in a public space where others can overhear.
    - E-communication examples *(follow your agency guidelines)*:
        - Use encrypted email.
            - Note: Email and files are automatically encrypted while in transit within the Google environment
                - Google for PHI and PPI - For Multco Employees
        - Use password protected attachments (required for files containing personally identifiable information from HMIS).
- Record storage & management - *(follow your agency guidelines)*
    - Check written ROI's for time limits to ensure permissions are still active.

******Please Note:* This general guidance is not legal advice, and users should seek their own legal counsel for specific questions.**

All sharing of HMIS information must comply with the HMIS Privacy & Security Notice and each agency's privacy notice. If you haven't read the Privacy & Security Notice, please do so.

FAQ

Other HMIS FAQ:

- See FAQ on HMIS Verbal ROIs at the bottom of this page.

What information can I share and receive if No HMIS ROIs have been completed?
Agencies should make their best effort to inform participants as to how their HMIS information will or may be shared. That is why:

- The HMIS Privacy Poster must be posted at all homeless services intake sites or shared with participants via another feasible means.
- The agency's privacy notice must contain, at a minimum, the entirety of the latest HMIS Privacy & Security Notice. The agency's privacy notice must also be posted to an agency's website and shared with participants upon request.

- HMIS providers must use the latest verbal HMIS ROI form to gain consent for data sharing *within* the HMIS system.
- The verbal ROI is used whenever possible in advance of Coordinated Access case conferencing.

With all that being said, **information from HMIS can be shared between agencies, even if there is no verbal HMIS ROI, *so long as certain conditions are met*.** Care coordination, program planning and case conferencing all justify sharing of HMIS information. For a full description of the conditions that enable the sharing of HMIS information, see the HMIS Privacy & Security Notice, linked above.

What information can I share and receive if only a verbal HMIS ROI has been completed?

As mentioned above, the verbal HMIS ROI is primarily used to find out if a client agrees to have their HMIS information shared with other agencies *within the HMIS system*. A verbal ROI is collected at each program enrollment and determines whether that particular enrollment and its associated information should be seen by other agencies within HMIS. If the verbal ROI is not "transacted" appropriately in HMIS or is transacted incorrectly, the information for that program enrollment will not be shared correctly in HMIS, which can limit visibility to other organizations and impact care coordination. *For more information on the relationship between the verbal ROI form and ROIs transacted in HMIS, see the FAQ: Verbal HMIS ROI.*

Note: The relationship between the verbal ROI form and data sharing within HMIS will change significantly once Multnomah County replaces its current HMIS with a new one called Clarity Human Services. As of this writing, the Clarity HMIS is scheduled to be fully implemented as early as Spring, 2027. To request updates on the HMIS Replacement project, email hmishelp@multco.us.

Multnomah agencies also use the verbal HMIS ROI to document consent for Coordinated Access (CA) data sharing, both inside and outside of HMIS. Typically, if a client does not give permission to share their CA information via the verbal ROI, that information is not shared in CA lists or as part of CA case conferencing. However, in lieu of a completed ROI and even in certain circumstances where a participant declines CA data sharing, someone's HMIS information may be shared outside HMIS, so long as the conditions of the Privacy & Security Notice (linked above) are met.

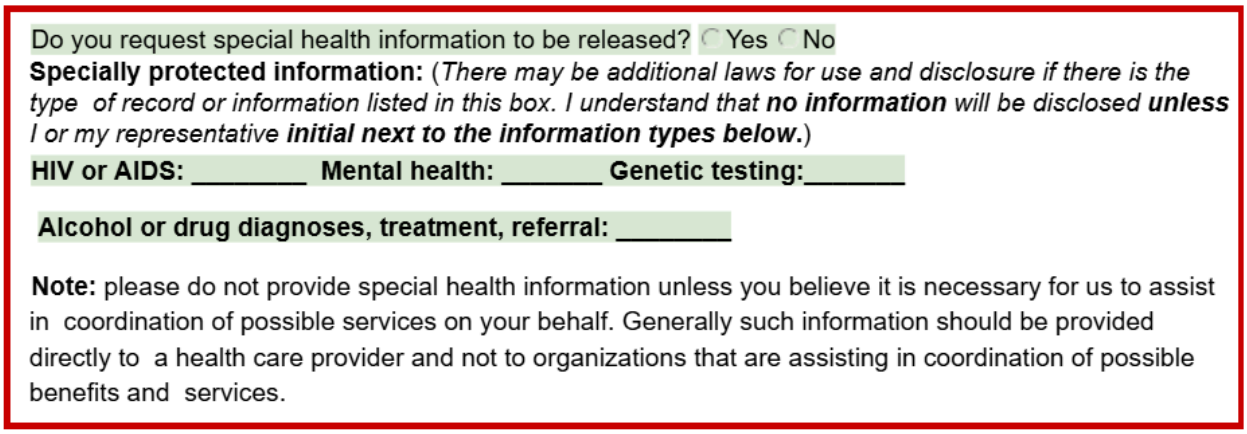
What information can I share and receive if a written ROI has been signed?

A release primarily serves to allow healthcare and disability service providers ("covered-entities") to share information with HMIS Users ("non-covered entities"). If a

written release has been signed, HMIS Users can share and receive the information outlined in that release.

Be careful to read releases carefully as not all ROI's allow all information to be shared. Certain types of information require additional levels of permission to share.

Example of Special Allowances from an ROI



Do you request special health information to be released? ○ Yes ○ No

Specially protected information: (*There may be additional laws for use and disclosure if there is the type of record or information listed in this box. I understand that* ***no information*** *will be disclosed* ***unless*** *I or my representative* ***initial next to the information types below.***)

HIV or AIDS: _____ Mental health: _____ Genetic testing:_____

Alcohol or drug diagnoses, treatment, referral: _____

Note: please do not provide special health information unless you believe it is necessary for us to assist in coordination of possible services on your behalf. Generally such information should be provided directly to a health care provider and not to organizations that are assisting in coordination of possible benefits and services.

Is health information considered PHI (e.g. subject to HIPAA regulations) if the organization is a non-HIPAA covered entity? - Health information held by organizations not covered by HIPAA (such as non-healthcare employers, apps, or websites) is generally not considered Protected Health Information (PHI) under the HIPAA Privacy Rule. While sensitive, this data is regulated by other laws,**What is a HIPAA-Covered entity** - A HIPAA covered entity is an organization or individual that must comply with HIPAA regulations, including healthcare providers, health plans, and healthcare clearinghouses that handle protected health information (PHI). They include doctors, hospitals, pharmacies, clinics, and insurers who conduct electronic transactions like billing.

Glossary

VAWA - The Violence Against Women Act (VAWA) is a 1994 U.S. federal law that provides protections, services, and legal rights to victims of domestic violence, sexual assault, dating violence, and stalking

HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law designed to protect sensitive patient health information from being disclosed without consent. It establishes national standards for handling Protected Health

Information (PHI), requiring healthcare providers, plans, and clearinghouses to secure data.

HIPAA Covered Entity - Organizations or individuals required to protect Protected Health Information (PHI). Examples include

- Healthcare Providers: Doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies that conduct standard electronic transactions (like insurance claims or eligibility inquiries).
- Health Plans: Health insurance companies, employer-sponsored health plans, and government programs like Medicare and Medicaid.
- Health Care Clearinghouses: Third-party intermediary that securely processes and standardizes medical billing data between healthcare providers and insurance payers.

Non-HIPAA Covered Entity - Organizations or individuals that handle health data but are not bound by HIPAA Privacy or Security Rules. Instead of HIPAA, client data privacy at these organizations is generally governed by HUD privacy standards through the Homeless Management Information System (HMIS).
Examples include

- State and Local Human Service Agencies: Departments managing income assistance, welfare programs (e.g., TANF), or SNAP/food stamps.
- Homelessness Service Providers: Community-based organizations operating residential facilities providing temporary shelter, emergency shelters, food service and case management without direct medical care.

PHI - Protected Health Information (PHI) is any identifiable information about a patient's health, treatment, or payment, created or maintained by covered entities under HIPAA. It covers past, present, or future physical/mental health data, including names, records, and identifiers in any form—written, electronic, or verbal
PII - Personally Identifiable Information (PII) is any data that can be used to distinguish, trace, or identify an individual's identity, either directly (e.g., name, SSN) or indirectly when combined with other personal or identifying information (e.g., birthdate, address). It includes sensitive data (e.g., medical records) and non-sensitive data (e.g., ZIP code).