Authorized & Unauthorized Requests for HMIS Data Disclosure

Bitfocus

This document guides frontline staff and Continuum of Care (CoC) policymakers responding to requests for Homeless Management Information System (HMIS) data. This guidance applies to all Covered Homeless Organizations (CHOs), including HMIS lead agencies, CoC-funded service providers, and any organization with access to or responsibility for HMIS data under federal regulations. It is designed to help you make informed decisions that protect client privacy while facilitating the necessary sharing of data.

Question 1: What type of data is being requested?

- **Aggregate or De-Identified Data:** Aggregate or de-identified data that does not contain Protected Personal Information (PPI) (e.g., anonymous statistics or service counts) may be shareable depending on the purpose of the request. De-identification requires robust processes to prevent re-identification through reasonably foreseeable methods.

- **Protected Personal Information (PPI):** Client-level information that identifies or could be used to identify a client is considered high-risk to share. This includes (but is not limited to) name, date of birth, Social Security Number, zip code, program entry/exit date, unique personal identification numbers, etc. HMIS uses this term to describe information which corresponds to what other federal regulations often refer to as Personally Identifiable Information (PII).

The shareability of data depends on the purpose of the request and the identity of the requester.

Question 2: Who is making the request?

	Proceed to Question 3?	Notes
The client	Always	Clients have an affirmative right to inspect and obtain a copy of their own PPI.
An HMIS-participating agency	Yes, with valid consent or data-sharing agreement	Sharing is generally covered by the CoC's Privacy Notice, which clients acknowledge upon entry. An explicit Release of Information (ROI) is typically needed for sharing more detailed information.
A government oversight entity (HUD, CoC lead agency, etc.)	Yes	Allowable for compliance or reporting.
An external organization (hospital, school, etc.)	Only with explicit, written client consent (ROI) or specific legal authority (e.g., court order)	Treat as high-risk. Formal, pre-approved data sharing agreements may also permit sharing if compliant with standards.
Law enforcement	Only with a subpoena or court order, or in a true emergency	Never release PPI without legal process unless it's a "serious and imminent threat to health or safety." Always consult legal counsel unless agency policy explicitly outlines the emergency procedure.
A researcher or evaluator	Only with de-identified data, or with explicit client consent (ROI) and a formal written research agreement	De-identified data is preferred. If PPI is necessary, it requires client consent and a formal written research agreement, and often Institutional Review Board (IRB) approval. The IRB reviews research ethics.
Funders (public or private)	Depends on the purpose	Routine reporting to funders for program operations and outcomes is generally authorized and often required by contract or law, typically involving aggregate or de-identified data. PPI should only be shared if explicitly required by law or contract, adhering to the "minimum necessary" principle.
Other	Unauthorized	Do not share information without explicit client consent or legal authorization.

Question 3: What is the Purpose of the Request

	Authorized?	Notes
Client accessing their own data	**Authorized**	Verify identity and follow relevant agency processes.
Service coordination or referral	**Authorized with consent**	Disclosures for service coordination or referral with HMIS-participating providers are generally authorized if outlined in the CoC's Privacy Notice and the client has consented to HMIS participation. An explicit ROI may be needed for sharing more detailed information or when sharing with non-HMIS participating agencies.
Required reporting	**Authorized**	Only share required information, typically aggregate or de-identified data.
Program evaluation	**Authorized if in contract or with consent/agreement**	For internal program evaluation, PPI may be used if permitted by the CoC's Privacy Notice and covered by a formal agreement. For external research, de-identification is preferred. If PPI is necessary, it requires explicit client consent (ROI) and a formal written research agreement.
Legal order or subpoena	**Authorized**	Consult with legal counsel and only release the minimum necessary information as legally required.
Emergency (Serious Threat to Health or Safety)	**Authorized for limited purposes**	Permitted if the CHO believes, in good faith, the disclosure is necessary to prevent or lessen a "serious and imminent threat to the health or safety of an individual or the public in general". This must be consistent with legal and ethical standards. Agencies should have pre-established policies for such scenarios.
Service payment/ reimbursement	**Authorized**	Permitted if outlined in the CoC's Privacy Notice and for minimum necessary purposes.
Administrative functions (audit, oversight, etc.)	**Authorized**	Permitted if outlined in the CoC's Privacy Notice and for minimum necessary purposes.
Research	**Only authorized to an Institutional Review Board with consent**	De-identified data is preferred. If PPI is necessary, it requires client consent and a formal written research agreement.
Other	**Unauthorized**	Do not share information without explicit consent or legal authorization.

Before moving on...

Stop and ask yourself:

1. Do I know who is requesting the information?
2. Do I understand why they want it?
3. Do I have the authority or client consent to share it?

⚠️ If you're unsure, stop and consult with your HMIS Lead, supervisor, privacy officer, and/or legal counsel.

Question 4: What should you do?

- **If Authorized**... Share the minimum necessary data, ensuring it's done through secure methods, and document the request and disclosure.
    - **Minimum Necessary:** Only share the specific PPI elements required for the stated, authorized purpose. If aggregate or de-identified data suffices, PII should not be shared.
    - **Secure Methods:** Use encrypted email, secure portals, secure file transfer protocols, or password-protected documents. Avoid sending or receiving unencrypted emails, faxes, or disclosing information verbally in public spaces. Consult your agency's IT and security policies.
    - **Documenting Requests:** Documentation should include the date of the request, the requestor's identity, the stated purpose, the specific data requested, the data shared (or the reason for denial), the method of sharing, and the identity of the staff member who handled it. For ROI, document start and end dates, verbal consent (and witness), and backdating if applicable.
- **If Unauthorized or Unclear**... Decline the request, immediately refer to the HMIS lead and/or a supervisor, and document both the request and response. For any legally mandated request (e.g., subpoena or court order) or if in doubt, always consult with agency legal counsel.

When in doubt, do not disclose – consult your HMIS Lead and/or supervisor.

Always document.