HMIS DATA USES AND DISCLOSURES

RELEASED: OCT 2024

UPDATED: NOV 2024

Uses and disclosures are either ***required*** (e.g., participants' access to their own information, oversight of compliance with the HMIS data privacy and security standards) ***or permitted by*** HUD (e.g., to provide services, reporting to funders). HUD's required and permitted uses and disclosures must be stated in the CoC's Privacy Notice.

HUD understands guidance may change local policies and practices that have been implemented under any previous guidance. If this guidance poses significant barriers to further HMIS implementation work, HUD recommends that you request HUD Technical Assistance (TA).

If TA resources are available and your request is approved, a HUD TA provider can offer on-call or on-site TA, depending on the complexity of the need. Submit your TA request through the **HUD Exchange TA Portal**. Grantees should work in partnership with project sponsors to coordinate project sponsor TA requests. You can find community examples of forms used for HMIS governance, privacy and consent purposes by visiting this website.

The table below lists both required and permitted uses and disclosures discussed in the 2004 HMIS Data and Technical Standards. The table offers best practices and recommendations for communities to consider when assessing their privacy policies and procedures. ***Note: State and Local laws may differ from this guidance; the more restrictive guidance should be implemented.***

Table 1.1: Required And Permitted Uses and Disclosures

TYPE OF USE OR DISCLOSURE	REQUIRED OR PERMITTED
To provide or coordinate services to an individual	Permitted
For functions related to payment or reimbursement for services	Permitted
To carry out administrative functions, includes, but is not limited to, legal, audit, personnel, oversight and management functions	Permitted
For creating de-identified datasets from Personally Identifiable Information (PII). This means stripping the PII entirely from the records prior to providing information. De-identified datasets mean the records cannot be matched to nor re-identified using any other alternate data source.	Permitted
To avert a serious threat to health or safety, including about victims of abuse, neglect or domestic violence	Permitted

TYPE OF USE OR DISCLOSURE	REQUIRED OR PERMITTED
For research purposes	Permitted with significant conditions and limitations.
For law enforcement purposes.	Permitted with significant conditions and limitations

Table 1.1: Best Practices and Recommendations

Include the participant's rights, the ways in which information may be used or disclosed (without written consent), a list of situations in which consent is required, the provider's responsibility to protect and secure participant information, and how the notice can be amended.

Place a sign at data collection points explaining why information is being collected and how to obtain the Continuum of Care's (CoC's) Privacy Notice.

Have a legal advisor review privacy practices and determine how other local, state and federal laws impact a provider's privacy and security requirements.

You can and should amend the Privacy Notice if it doesn't include all allowable uses and disclosures. Changes should go through the CoC governing body to work through amendments and get approvals. CoC agencies must adopt and implement updates to this policy.

HUD CoC FAQ 3310

Table 1.1: Additional Notes

Data ownership or access questions should be addressed by the CoCs through any HMIS governance, policies, or agreements in place between associated parties.

HUD permits these uses and disclosures of PII without participant consent, provided that the uses and disclosures are listed in the CoC's Privacy Notice, if that use or disclosure does not violate other local, state or federal laws. Client consent is required if any of these uses and disclosures are not listed in the Privacy Notice.

A CoC may elaborate on or provide examples of these activities in its Privacy Notice, but that is not required. If examples are included in the Privacy Notice, they should be

marked as examples and not an exhaustive list of permitted uses and disclosures. These uses and disclosures come with significant conditions and limitations.

CoC Program interim rule Section 578.57 HMIS

Table 1.2: Required And Permitted Uses and Disclosures

TYPE OF USE OR DISCLOSURE	REQUIRED OR PERMITTED	BEST PRACTICES AND RECOMMENDATIONS	ADDITIONAL NOTES
Client access to their information	Required	Give the participant a copy of the Privacy Notice.	These disclosures are **required** regardless of inclusion in the CoC's Privacy Notice.
Disclosures for oversight of compliance with HMIS privacy and security standards	Required	Give the participant a copy of the Privacy Notice.	These disclosures are **required** regardless of inclusion in the CoC's Privacy Notice.
Other uses or disclosures not otherwise listed in the 2004 HMIS Data and Technical Standards or in the CoC's Privacy Notice	Permitted with participant consent	Other uses and disclosures **require** participant consent. Consent may be captured verbally or in writing, electronically or manually.	-

COVERED HOMELESS ORGANIZATION REQUIREMENTS

The 2004 Notice lists requirements of Covered Homeless Organizations (CHO) to ensure the HMIS security and privacy requirements of the Notice are operationalized in a consistent and standardized manner by all CoCs. Below is a breakdown of the specific elements of privacy and security for CHOs and CoCs to implement as part of their overall HMIS management strategies, the baseline requirements (if any), and current additional recommendations to ensure HMIS implementations are up to date with the latest information technology security best practices.

Table 2: Privacy and Security Requirements for CoCs and Covered Homeless Organizations (CHOs)

REQUIREMENT	BASELINE REQUIREMENTS	ADDITIONAL RECOMMENDATIONS
A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A CHO must maintain permanent documentation of all privacy notice amendments.	Indicate in the Privacy Notice that changes are retroactively applied; include this in any update of the Privacy Notice it is required; and maintain amendments of the Privacy Notice on file at HMIS Lead.	-
A CHO must publish a Privacy Notice describing its policies and practices for processing of PII and must provide a copy of its Privacy Notice to any individual upon request.	Include uses and disclosures of data per the table above in this document.	Add additional protections to PII, such as hashing, secure file transfer protocols, and other ways the CHO can ensure security and privacy for already vulnerable people experiencing homelessness.

REQUIREMENT	BASELINE REQUIREMENTS	ADDITIONAL RECOMMENDATIONS
A CHO must allow an individual to inspect and to have a copy of any PII about the individual.	Include this specific provision in the CoC's Privacy Notice and operationalize the process for providing it to clients in HMIS Policies and Procedures. Make sure all CHO and CoC staff handling HMIS data know how to do the process if requested.	Ensure the CoC or CHO can provide services to help translate privacy information if needed.
A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices.	Create a process that allows clients to provide feedback.	Commit to additional privacy (optional) (e.g., formal privacy training, appeals process, designate privacy officer).
A CHO must apply system security provisions to all the systems where PII is stored.	Virus Protection, Firewalls.	Commit to additional security (optional) (e.g., complex passwords, public access requirements, Virtual Private Network).
A CHO must copy all HMIS data on a regular basis to another medium (e.g., tape) and store it in a secure off-site location where the required privacy and security standards would also apply.	This requirement ensures that situations such as fires or natural disasters do not cause long-term record destruction.	This is often embedded in HMIS software contracts, but the CHO is responsible for ensuring it is part of the overall HMIS management protocol and CHO can test regularly (via contract monitoring).
A CHO must apply application security provisions to the software during data entry, storage and review or any other processing function.	Security must be applied to HMIS applications.	Strict password rules (e.g., 10+ character minimums, use of symbols, numbers, lowercase and uppercase letters, no common words, no repeating passwords).

REQUIREMENT	BASELINE REQUIREMENTS	ADDITIONAL RECOMMENDATIONS
A CHO must secure any paper or other hard copy containing PII that is either generated by or for HMIS.	Hard copies must be supervised at all times in public areas and secured otherwise. Per the FAQs of retention and disposal, hard copies of HMIS records must be treated the same as electronic HMIS records, and both must be destroyed after seven years of retention.	A CHO must ensure the HMIS software vendor that secures or maintains the HMIS data is following retention policies.
A CHO must encrypt all HMIS data that are electronically transmitted over the Internet, publicly accessible networks, or phone lines to current industry standards.	Must use at least 128-bit encryption. Resource for Data Encryption	-