

Title: 2.1 Data Privacy & Security Policies

---

Prepared By: CAFTH

Reviewed By: CE Ad Hoc Committee

---

Approved By:

Date Approved:

---

CE process partners and all participating agencies contributing data to CE must ensure participants' data are secured regardless of the systems or locations where participant data are collected, stored, or shared, whether on paper or electronically. Additionally, participants must be informed about how their data is being collected, stored, managed, and potentially shared, with whom, and for what purpose.

*Client Information and Confidentiality Process*

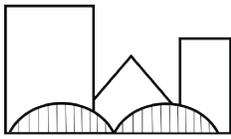
Before an assessment is completed, CE staff administering the assessment must review the release of information form (included in the Appendix) on the front of the assessment with clients. This form identifies what data will be collected, where data will be stored/managed, how data will be used for the purposes of helping the participant obtain housing and assistance and for other administrative purposes, and what data will be shared with others (if the participant consents to such data sharing).

All data, files, records, and documentation are confidential information and are only shared with written permission from the client. All client data collected during the Coordinated Entry process will only be shared among CE Community Organizations who have signed a confidentiality agreement with the CE Lead Agency. The confidentiality agreement states all recorded data will only be shared with designated staff for the purposes of CE management, participant care coordination, CE evaluation, and other administrative purposes. Upon review of the release of information and the purpose of the assessment, clients must then sign the consent form or verbally notify that they understand and agree to participate in the assessment.

Additionally, protected data such as that of a specific disability or diagnosis will not be used to prioritize specific households above others. Prioritization policies and procedures for clients in CE are outlined in Section 1.4.

*HMIS and Client Data Security*

If clients consent to having their data shared, their information will be stored within HMIS. CE staff should thoroughly explain the process of storing client data in HMIS, and the data security standards in place to protect client data. Assessors should also



ensure that clients understand that their choice regarding their information being stored in HMIS will not affect their access to housing resources.

At any time, a client can request to view their information or request to have their information removed from HMIS. To get their information removed, they must make a direct request to the HMIS Lead Agency to have their information removed. The Lead Agency will then remove their information. If a client desires or requires assistance to complete this request, service providers are encouraged to assist clients with completing their request. The same HMIS data privacy and security protections will be applied to the By-Name List as prescribed by HUD for HMIS practices in the HMIS Data and Technical Standards<sup>1</sup>.

In line with HUD regulations,<sup>2</sup> the CoC complies with mandatory disclosures of any oversight with compliance of HMIS privacy and security standards.

#### *Client's Right to Refuse Questions*

Before completing any assessment, it is the responsibility of the service provider to inform the client of their right to refuse any individual questions during the assessment and ensure clients understand that doing so does not affect their ability to access housing programs. Under no circumstance does refusal of information or request to have information removed make any participant ineligible for services unless the information is necessary to establish or document program eligibility per applicable program regulation.

#### *Domestic Violence and Privacy*

The Domestic Violence population comes with its own set of privacy and confidentiality standards. Recipients of Violence Against Women Act (VAWA) funding and all agencies that participate in Coordinated Entry are prohibited from disclosing personally identifiable information without the participant's written consent.

Client's fleeing domestic violence can have their information entered into a VAWA-compliant comparable database but will not be entered into the HMIS. Comparable databases collect aggregate data with no identifying information being stored or reported, which makes client information entered unidentifiable to others.

---

<sup>1</sup> Department of Housing & Urban Development. (2004) Homeless Management Data and Technical Standards Final Notice. Retrieved from: <https://files.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf>

<sup>2</sup> Coordinated Entry: Management and Data Guide. (2018). *Chapter 2: data privacy and security*. Retrieved from: <https://files.hudexchange.info/resources/documents/coordinated-entry-management-and-data-guide.pdf>