DC HMIS PRIVACY POLICY

VERSION 2.1
EFFECTIVE DATE: JANUARY 1, 2021

SUMMARY

This policy describes the privacy policy and procedures of the DC HMIS related to the privacy policy. These policies and procedures cover the processing of protected personal information for clients of participating agencies of the DC HMIS. This policy covers all personal information that is maintained within the DC HMIS.

Protected Personal Information (PPI) is any information about a client that:

a. Allows identification of an individual directly or indirectly; and
b. Can be manipulated by a reasonably foreseeable method to identify a specific individual;

OR

c. Can be linked with other available information to identify a specific client.

When this policy refers to personal information, it means PPI.

This policy is in accordance with the *Homeless Management Information Systems Data and Technical Standards* issued by the U.S. Department of Housing and Urban Development and is consistent with requirements outlined in the DC Homeless Services Reform Act and other applicable local laws.

The Lead Agency may amend this policy and/or change procedures at any time. Amendments may affect personal information that was obtained before the effective date of the amendment. The new policy will be posted at the Lead Agency's website, www.community-partnership.org, at least 30 days prior to taking effect.

Partner Agencies will provide a written copy of this privacy policy to any individual that requests one. The Lead Agency also maintains a copy of this policy on its website located at www.community-partnership.org.

COLLECTION OF PERSONAL INFORMATION

Personal information will be collected only when appropriate to provide services, or for another specific purpose of the agency where a client is receiving services. Or when it is required by law.

Personal information may be collected for these purposes:

- To provide or coordinate services for clients
- To find programs that may provide additional client assistance
- To comply with government or grant reporting obligations
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources.

Personal information must be collected with the knowledge and consent of clients. It is assumed that clients consent to the collection of this personal information as described in this notice when they seek assistance from an agency using HMIS and provide the agency with their personal information.

Personal Information about clients may also be collected from:

- Additional individuals seeking services with a client
- Other private organizations that provide services and participate in HMIS.

USE AND DISCLOSURE OF PERSONAL INFORMATION

These policies outline how information may be used and disclosed by the Lead Agency on behalf of the DC Continuum of Care. Through the use of the Release of Information, personal information is able to be shared among the various partner agencies participating in HMIS or with external data partners as outlined in the Release of Information. Personal information may be used or disclosed without client consent for the following purposes:

a. To provide or coordinate services for individuals to help them exit homelessness. To accomplish this goal, client data may be shared among HMIS-participating providers as well as with non-participating network partners – that is, agencies with which the Lead Agency, TCP, has a written data sharing agreement or HMIS Agency Agreement.
b. To carry out administrative functions such as audits, personnel, oversight, and management functions.
c. For research and statistical purposes. Personal information released for research and statistical purposes will be anonymous.
d. For academic research conducted by an individual or institution that has a formal relationship with the Lead Agency, TCP. The research must be conducted by an individual employed by or affiliated with the organization or institution. All research projects must be conducted under a written research agreement approved in writing by the Lead Agency. The written agreement must:
    - Establish the rules and limitations for processing personal information and providing security for personal information in the course of the research.
    - Provide for the return or proper disposal of all personal information at the conclusion of the research.
    - Restrict the additional use or disclosure of personal information, except where required by law.
    - Require that the recipient of the personal information formally agree to comply with all terms and conditions of the written research, and
    - Be substituted, when appropriate, by Institutional Review Board, Privacy Board or other applicable human subjects' protection institution approval.
e. When required by law. Personal information will be released to the extent that use or disclosure complies with the requirements of the law.
f. To avert a serious threat to health or safety if:
    - The use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
    - The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
g. To report to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect, or domestic violence, information about an individual reasonably believed to be a victim of abuse, neglect, or domestic violence. When the personal

information of a victim of abuse, neglect, or domestic violence is disclosed, the individual whose information has been released will promptly be informed, except if:

- It is believed that informing the individual would place the individual at risk of serious harm, or
- A personal representative (such as a family member or friend) who is responsible for the abuse, neglect, or other injury is the individual who would be informed, and it is believed that informing the personal representative would not be in the best interest of the individual as determined in the exercise of professional judgement.

h. For a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
    - In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer or a grand jury subpoena, if the court ordered disclosure goes through the Lead Agency, TCP, and is reviewed by the Executive Director for any additional action or comment.
    - If the law enforcement official seeks personal information, they must provide a subpoena and the subpoena must meet the following requirements:
        i. Be signed by a supervisory official of the law enforcement agency seeking the personal information.
        ii. Identify the personal information sought.
        iii. Be specific and limited in scope to the purpose for which the information is sought, and
        iv. Be approved for release by TCP's legal counsel after a review period of seven to fourteen days.
    - If it is believed that the personal information constitutes evidence of criminal conduct that occurred at the agency where the client receives services.
    - If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to a foreign head of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.
i. For a law enforcement or another public official authorized to receive a client's personal information to conduct an immediate enforcement activity that depends upon the disclosure. Personal information may be disclosed when a client is incapacitated and unable to agree to the disclosure if waiting until the individual is able to agree to the disclosure will only be made if it is not intended to be used against the individual.
j. To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.
k. In the event of a public health emergency, personal information, including protected health information, may be disclosed to appropriate public health entities to support coordination measures to protect public health.

INSPECTION AND CORRECTION OF PERSONAL INFORMATION

Clients may inspect and receive a copy of their personal information maintained in HMIS. The agency where the client receives services will offer to explain any information that a client may not understand. If the information listed in HMIS is believed to be inaccurate or incomplete, a client may submit a verbal or written request to have their information corrected. Inaccurate or incomplete data may be deleted, or marked as inaccurate or incomplete and supplemented with additional information.

A request to inspect a copy of one's personal information may be denied if:

- The information was compiled in reasonable anticipation of litigation or comparable proceedings,
- The information was obtained under a promise of confidentiality and if the disclosure would reveal the source of the information, or
- The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information.

If a request for inspection access or personal information correction is denied, the agency where the client receives services will explain the reason for the denial. The client's request and the reason for the denial will be included in the client's record. Requests for inspection access or personal information correct may be denied if they are made in a repeated and/or harassing manner.

LIMITS ON COLLECTION OF PERSONAL INFORMATION

Only personal information relevant for the purpose(s) for which it will be used will be collected. Personal information must be accurate and complete to the furthest extent possible. Client files not used in seven (7) years may be made inactive in HMIS. The Lead Agency will check with partner agencies before making client files inactive. Personal information may be retained for a longer period if required by statute, regulation, contract, or another obligation.

LIMITS ON PARTNER AGENCY USE OF CLIENT INFORMATION

The DC HMIS is a partially open data system. This system allows for the ability for Partner Agencies to share client information in the event that a Release of Information is signed in order to coordinate services for clients. However, Partner Agencies may not limit client service or refuse to provide service in a way that discriminates against clients based on information the Partner Agency obtained from HMIS. Partner Agencies may not penalize a client based on historical data contained in HMIS.

Youth providers serving clients under the age of 18 must maintain HMIS client files that are not shared. Youth under the age of 18 may not provide either written or verbal consent to the release of their personally identifying information in HMIS.

COMPLAINTS AND ACCOUNTABILITY

Questions or complaints about the privacy and security policies and practices may be submitted to the agency where the client receives services. Complaints specific to HMIS should be submitted to the Agency Administrator and program director. If no resolution can be found, the complaint will be forwarded to the Lead Agency's HMIS Staff. If there is no resolution, the Lead Agency's Executive Director will oversee final arbitration. All other complaints will follow the agency's grievance procedure as outlined in the agency's handbook.

All HMIS users (including employees, affiliates, contractors, and associates) are required to comply with this privacy notice. Users must receive and acknowledge receipt of a copy of this privacy notice.