Tarrant County Homeless Coalition Privacy Policy

The Tarrant County Homeless Coalition (TCHC) HMIS Privacy Policy describes standards for the privacy of personal information collected and stored in the TCHC Homeless Management Information System (TCHC HMIS), as well as personal information collected for the purposes of the TCHC Coordinated Access System(TCHC CAS). The Privacy Policy (herein after referred to as "Policy") to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. This Policy defines the privacy standards that will be required of any organization within the TCHC CoC that records, uses, or processes personally identifiable information (PII) on clients at-risk of or experiencing homelessness for the TCHC HMIS or the TCHC CAS. Organizations must also comply with federal, state, and local laws that require additional confidentiality protections, where applicable. This Policy recognizes the broad diversity of organizations that participate in the TCHC HMIS and/or the TCHC CAS, and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations (e.g., such as those serving victims of domestic violence, HIV/AIDS and youth) may choose to implement higher levels of privacy standards because of the nature of the clients they serve and/or service provision. At a minimum, however, all organizations must meet the privacy standards described in this Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections. The following sections discuss the TCHC HMIS and the TCHC CAS privacy standards.

HMIS PRIVACY

The HMIS Governance Committee is responsible for establishing policies, procedures, and a monitoring plan pertaining to Privacy Notice; client authorization form (Release of Information); and electronic and paper documents containing personal identifying information (i.e. intake forms, assessment tools, By Name Lists, referral forms, etc.). HMIS staff must ensure that the HMIS software is configured correctly to ensure compliance with CoC established privacy policies and procedures and conduct monitoring for compliance with established policies, procedures, plans, and report deviations from privacy protocol according to an established channel of communication.

Participating Agencies must obtain informed, signed, or verbal consent prior to entering any client personal identifiable information into HMIS. Services will not be denied if a client chooses not to include personal information. Personal information collected about the client should be protected. Each Participating Agency and end user must abide by the terms in the HMIS Agency Participation Agreement (Appendix A) and HMIS User License Agreement (Appendix B). Client must sign the Authorization to Disclose Client Information form (Appendix F) or consent of the individual for data collection may be inferred from the circumstances of the collection. Clients that provide permission to enter personal information allow for Participating Agencies within the continuum to share client and household data. If client refuse consent, the end user should not include any personal identifiers (First Name, Last Name, Social Security Number, and Date of Birth) in the client record. For clients with refused consent, end user should include a client identifier, such as a client profile number, to recognize the record in the system. However, user should strive for client anonymity.

Each of the HMIS Partner Agencies must comply with the following uses and disclosures, as outlined in the HUD Data and Technical Standards: Notice for Uses and Disclosures for Protected Personal Information (PPI). A Partner Agency has the right to establish additional uses and disclosures so long as they do not conflict with approved uses and disclosures. See below for detailed information on Personally Identifiable Information and Protected Personal Information.

Privacy Notice Requirement: Each Partner Agency must publish a privacy notice that incorporates the content of the HUD Data and Technical Standards Notice. Agencies that develop their own privacy and security policies must allow for the de-duplication of homeless clients at the Continuum level. Participating Agencies shall uphold Federal and State Confidentiality regulations and laws that protect client records.

Approved Uses and Disclosures

Identifiable HMIS client data may be used or disclosed for case management, billing, administrative, and analytical purposes.

- Case management purposes include uses associated with providing or coordinating services for a client. As part of case management, the agency will share client information with other agencies based only on written client consent, or in the case of call center operations, explicit oral consent
- Billing uses include functions related to payment or reimbursement for services. An example might include generating reports for fundraising purposes
- Administrative purposes are uses required to carry out administrative functions, including but not limited to legal, audit, personnel, oversight, and management functions. An example would be analyzing client outcomes to evaluate program effectiveness
- Analytical purposes are functions that are related to analyzing client data to understand homelessness, including but not limited to creating de-identified protected personal information, understanding trends in homelessness and the needs of persons who are homeless, and assessing the implementation of the Continuum's Strategic Plan

Unless a client requests that his/her record remains hidden, his/her primary identifiers will be disclosed to other HMIS agencies. This will allow agencies to locate the client within the HMIS system when the client comes to them for services. This will allow the Continuum to determine how many people are

homeless in our region during any specified timeframe. Identifiable client information may also be used, or disclosed, in accordance with the HUD Data and Technical Standards for:

- Uses and disclosures required by law
- Aversion of a serious threat to health or safety (to include Covid-19)
- Uses and disclosures about victims of abuse, neglect, or domestic violence
- Uses and disclosures for academic research purposes
- Disclosures for law enforcement purposes in response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial office or a grand jury subpoena

Aside from the disclosures specified above, a client's protected personal information will be disclosed only with his/her written consent. Client information will be stored with personal identifiers for a period of seven years from the time it was last modified. Beyond that point, client information will be retained only in a de-identified format.

Other Allowable Uses and Disclosures

Provided below are additional uses and disclosures of information allowable by HUD standards. It should be noted that these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this standard modifies an obligation under applicable law to use or disclose personal information (Section 4.1.3, 2004 HMIS Data and Technical Standards).
A CHO may use or disclose PII when required by law to the extent that the disclosure complies with and remains within the boundaries of said law, in response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer, or a grand jury subpoena. A CHO must take immediate actions to notify TCHC about all legal disclosures. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO may contact TCHC before approving any disclosure.

A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:

- The CHO, in good faith, believes 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
- The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat

A CHO must take immediate actions to notify TCHC about all legal disclosures. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO must contact TCHC before approving any disclosure.

A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII to a law enforcement official under any of the following circumstances:

- In response to a request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PII disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics

- If the official is an authorized federal official seeking PII for the provision of protective services to the President or other authorized persons OR for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others)

All CHOs must comply with the baseline privacy requirements described here with respect to data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO may adopt additional substantive and procedural privacy protections that exceed the baseline requirements for each of these areas in its privacy notice. A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PII. When PII is shared between organizations, responsibilities for privacy and security may be allocated between the organizations (Section 4.2, 2004 HMIS Data and Technical Standards). All CHO policies regarding privacy requirements must at a minimum include the criteria in this document. Additional requirements may be added at the discretion of each CHO.

HIPAA

The Agency will abide specifically with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and corresponding regulations passed by the U.S. Department of Health and Human Services. In general, the regulations provide consumers with new rights to control the release of medical information, including advance consent for most disclosures of health information, the right to see a copy of health records, the right to request a correction to health records, the right to obtain documentation of disclosures of their health information, and the right to an explanation of their privacy rights and how information may be used or disclosed. The current regulation provides protection for paper, oral, and electronic information.

The HMIS standards and the HIPAA standards are mutually exclusive. An organization that is covered under the HIPAA standards is not required to comply with the HMIS privacy or security standards, so long as the organization determines that a substantial portion of its protected information about homeless clients or homeless individuals is indeed protected health information as defined in the HIPAA rules.

HIPAA standards take precedence over HMIS because HIPAA standards are finely attuned to the requirements of the health care system; they provide important privacy and security protections for protected health information; and it would be an unreasonable burden for providers to comply with and/or reconcile both the HIPAA and HMIS rules. This spares organizations from having to deal with the conflicts between the two sets of rules. HIPPA rules are triggered by the type of entity managing the data rather than health information. HUD funded organizations participating in HMIS are not subject to HIPPA regulations. There are no data elements in HMIS that would require HIPPA compliance.

Protection of Client Privacy

The Agency will comply with all applicable federal and state laws regarding protection of client privacy as well as all policies and procedures established by TCHC pertaining to protection of client privacy. Further, the Agency will comply specifically with federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal rules prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not

sufficient for this purpose. The Agency understands that the federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse cases.

Client Confidentiality

The Agency agrees to provide a copy of the TCHC CoC Data Privacy Notice to each consumer. The Agency will obtain each consumer's consent to collect data on the Client Consent of Data Collection (or an acceptable Agency-specific alternative) form. If consent is not given, then the Agency will enter consumer information as "anonymous". The Agency will provide a verbal explanation of the TCHC CoC HMIS and arrange for a qualified interpreter/translator in the event that an individual is not literate in English or has difficulty understanding the Data Privacy Notice or Client Consent of Data Collection form. The Agency acknowledges that clients who choose not to consent to release of information cannot be denied services for which they would otherwise be eligible. The Agency will secure a completed Client Revocation of Release of Information Consent Form (REV) for these clients.

The Agency will not solicit or enter information from clients into the TCHC CoC HMIS databases unless it is essential to provide services or conduct evaluation or research. The Agency will not divulge any confidential information received from the TCHC CoC HMIS to any organization or individual without proper written consent by the client on the Client Release of Information Consent Form (ROI) unless otherwise permitted by applicable regulations or laws. The Agency agrees to place all Client Release of Information Consent forms related to the TCHC CoC HMIS in a file to be located at the Agency's business address and that such forms will be made available to TCHC for periodic audits. The Agency will retain these TCHC CoC HMIS-related Release of Information Consent forms for a period of 7 years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.

The Agency will ensure that all persons who are issued a User Identification and Password to the TCHC CoC HMIS System abide by the Participation Agreement, including all associated confidentiality provisions. The Agency will be responsible for oversight of its own related confidentiality requirements. The Agency agrees that it will ensure that all persons issued a User ID and Password will complete a formal training provided by TCHC on privacy and confidentiality and demonstrate mastery of that information, prior to activation of their User ID. The Agency acknowledges that ensuring the confidentiality, security and privacy of any information downloaded from the system by the Agency is strictly the responsibility of the Agency.

Personally Identifiable Information and Protected Personal Information

The information below summarizes client data categories and related notification/consent rules that relate to each data category.

Client Data Categories	Notification, Consent and Data Sharing Procedures
<u>Primary Identifiers:</u> • Name and Aliases • Birth Date	<u>Open Client Record:</u> If the client does not ask to hide his/her identifiers, the primary identifiers will be available to all HMIS users in the Client

• Gender • Social Security Number • Family/Relationship Information • Client Veteran Status	Search to locate an existing client. None of the other client information will be viewable, except as described below Closed Client record: If a client asks to hide his/her primary identifiers, the record will appear on the Client Search List only for the originating agency. It will be hidden to all other agencies. Some system-level users will have access to hidden records for system administration purposes
General Client Information (Demographics, Entry/Exit, and Service Transactions): • Ethnicity • Race • Services Provided • Program Enrollment (Entry/Exit)	Open Assessment: With a signed release of information (ROI), these data can be shared with HMIS users from partner agencies by opening/unlocking the Demographics assessment and relevant Entry/Exit and Service Transactions Closed Assessment: If written consent is not provided, this information is accessible only within the originating agency and some system-level users for system administration purposes
Protected Information: • Housing History • Income/Benefits/Employment • Disability Information • Mental Health Assessment • Substance Abuse Assessment • HIV/AIDS Information • Domestic Violence Information	Protected Information: Generally, this information is available only within the originating agency to users that have an authorized access level and to authorized, system-level users for system administration purposes. Any other sharing of this data should be limited to specific Partner Agencies and requires signed consent from the client

Privacy and HMIS

Disclosures required by law: A CHO may use or disclose PPI when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law. Disclosures to avert a serious threat to health or safety: Uses and disclosures to avert a serious threat to health or safety. A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PPI if: (1) the CHO, in good faith, believes 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 (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat. Any information maintained by or for a member of the Tarrant County Homeless Coalition or other Covered Homeless Organization about a living homeless client or homeless individual which:

- Identifies, either directly or indirectly, a specific individual
- Can be manipulated by a foreseeable method to identify a specific individual; or
- Can be linked with other available information to find a specific individual (Section 4.1.1, 2004 HMIS Data and Technical Standards)

A CHO will enter in to HMIS a required set of data variables for each client, including all universal and program specific data elements, which are detailed in the HUD HMIS Data and Technical Standards (see Appendix A for list of Data Elements). All HMIS End Users are trained in the appropriate and accurate procedures for entering PII into HMIS. This training is provided by the Tarrant County Homeless Coalition Department of Information Services.