Cambridge, MA Continuum of Care

Homeless Management Information System

Policies and Procedures Manual

October 2020

HOMELESSNESS MANAGEMENT INFORMATION SYSTEM (HMIS) POLICIES AND PROCEDURES MANUAL

This manual is developed by the HMIS Lead and authorized by the HMIS Working Group.

CHMIS Lead Agency Contact Information

CHMIS Information Website	https://cambridgecoc.org/hmis/
CHMIS Training Website	https://cambridgetrain.clarityhs.com/login
CHMIS Login	https://cambridge.clarityhs.com
HMIS System Administrator	Marianne Colangelo City of Cambridge Continuum of Care Department of Human Service Programs 51 Inman Street Cambridge, MA 02139 mcolangelo@cambridgma.gov
HMIS Data Coordinator	Laura Vitagliano Cambridge MultiService Center lvitagliano@cambridgema.gov

Version History		
Date	**Author**	**Description**
10/19/2011	DHSP, P&D	First draft to be distributed to HMIS Committee
11/10/2011	DHSP, P&D	Draft for distribution to full HSPC
12/30/2012	DHSP, P&D	Glossary of terms added
1/13/2014	DHSP, P&D	Removal of HPRP and PULSE references; addition of ESG CAPER information; replaced SHP & SPC with CoC
12/8/2014	DHSP, P&D	Updated to reflect 2014 Data Standards
6/27/2016	DHSP, P&D	Updated to reflect change in data elements (2015), HMIS Vendor, Client Consent procedure and System Performance Measure report requirement.
10/08/18	DHSP, P&D	Updated to reflect change in data elements (2017), automation of user account expiration, data quality procedure.
9/10/2020	DHSP, P&D	Complete re-write of document.

ABOUT THIS DOCUMENT

This document serves as the minimum standards of participation in the Cambridge HMIS and represents general best practices. This set of HMIS Policies and Procedures documents the Cambridge Continuum of Care's operation of its HMIS and acts as a guide to its continuing operation in compliance with the CoC and ESG Regulations and Interim Rules.

Operational standards in this document are not intended to supersede grant specific requirements and operating procedures as required by funding entities. PATH, HOPWA, and VA providers have operating rules specific to HHS and VA. Cambridge HMIS will update this document at any time when necessary due to HUD or CoC changes. The latest versions of the HUD HMIS Data Standards Manual and Data Dictionary are the basis for all programming specifications and requirements of HMIS. Updates will be brought to the HMIS Working Group for approval. Upon approval, updates to this document will be announced to all Agency Administrators via email and posted on the Cambridge HMIS website. The most recently updated version of this document is the only version that is considered valid and supersedes all previous versions.

PROJECT SUMMARY

Background

In order to accomplish the vision of homelessness being rare, brief and non-recurring in Cambridge, we must know the scope of the problem, understand the characteristics of individuals and families who find themselves homeless in our community, and be able to identify which strategies are beneficial toward our goal and which are not.

A Homeless Management Information System (HMIS) is the information system designated by a local Continuum of Care (CoC) to comply with the requirements of CoC Program Interim Rule (24 CFR 578). It is a locally administered data system used to record and analyze client, service and housing data for individuals and families who are homeless or at risk of homelessness. Client data is maintained on a central server, which holds all information in an encrypted state.

HMIS is a valuable resource because of its capacity to integrate and un-duplicate data across projects in a community. Aggregate HMIS data can be used to understand the size, characteristics, and needs of the homeless population at multiple levels: project, system, local, state, and national. The Longitudinal Systems Analysis (LSA) report, produced from a CoC's HMIS and submitted annually to HUD, provides HUD and CoCs with critical information about how people experiencing homelessness interact with the system of care. This report could not be

produced if communities were not able to provide HUD with reliable, aggregate data on the clients they serve.

The Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act codifies in law certain data collection requirements integral to HMIS. The HEARTH Act requires that HUD ensure operation of and consistent participation by recipients and subrecipients in HMIS.

In 2010 the U.S. Interagency Council on Homelessness (USICH) affirmed HMIS as the official method of measuring outcomes in its Opening Doors: Federal Strategic Plan to Prevent and End Homelessness. Since then, many of the federal agencies that provide McKinney-Vento Act and other sources of funding for services to specific homeless populations have joined and are working with HUD to coordinate the effort.

In addition, the HEARTH Act required HUD to establish standards related to HMIS, including standards related to encryption of the data collected and the rights of persons receiving services under the McKinney-Vento Act. On December 9, 2011, HUD continued its process of implementing the HEARTH Act by publishing 24 CFR Parts 91, 576, 580, and 583 - the Homeless Management Information Systems Requirements. This proposed rule added a new part to the Code of Federal Regulations to regulate the administration of HMIS and the collection of data using HMIS, as provided for by the HEARTH Act (24 CFR part 580). The proposed rule also makes corresponding changes to HUD's regulations for Consolidated Submissions for Community Planning and Development Programs, at 24 CFR part 91; the Emergency Solutions Grants program, at 24 CFR part 576; the Shelter Plus Care Program, at 24 CFR part 562; and the Supportive Housing Program, at 24 CFR part 583. The proposed rule implements the HMIS requirement in the HEARTH Act and makes mandatory the practices that HUD previously provided as guidance.

HMIS is now used by the federal partners and their respective programs in the effort to end Homelessness, which include:

- U.S. Department of Health and Human Services (HHS)
- U.S. Department of Housing and Urban Development (HUD)
- U.S. Department of Veterans Affairs (VA)

The HMIS Data Standards provide communities with baseline data collection requirements developed by each of these federal partners. The HMIS Data Standards Manual is designed for CoC's, HMIS Lead Agencies, HMIS System Administrators, and HMIS End Users to help them understand the data elements that are required in an HMIS to meet participation and reporting requirements established by HUD and the federal partners.

HUD is responsible for coordinating the collection of data, overseeing HMIS rules and regulations, and reporting to Congress through the Annual Homeless Assessment Report (AHAR), and will continue to manage the HMIS regulations, provide support and guidance to local CoCs and HMIS Lead Agencies, and provide guidance to users in collaboration with the

federal partner agencies. The 2014 release of the Data Dictionary and Manual was the first joint publication of HUD and the federal partners and is intended to provide guidance to communities around federal expectations for HMIS. The HMIS Data Standards Manual was updated most recently in June of 2020.

Cambridge's Continuum of Care

The Cambridge Continuum of Care includes all the geography within the City of Cambridge, Massachusetts. The Cambridge CoC is a system of housing and services that provides a broad range of homelessness prevention and intervention services to the community. The City of Cambridge Department of Human Service Programs (DHSP) is the designated Collaborative Applicant for the CoC and works to coordinate the community's compliance with CoC Program requirements specified in 24 CFR 578. The Collaborative Applicant is the eligible applicant that submits the annual CoC Consolidated Application to the HUD for funding on behalf of the CoC.

Vision for Cambridge HMIS

The vision for this system in Cambridge is that clients, agencies, and the community benefit from a streamlined approach to referrals, intakes, and assessments across the entire service delivery system. The goal of our HMIS is to offer the following benefits:

- Ensured regulatory compliance with HEARTH Act and HUD system requirements as outlined in the current HMIS Data Technical Standards;
- Coordinated services across agencies, programs and services that is designed to limit clients' need to repeat their story;
- The ability to track and measure outcomes and effectiveness of the programs operating within the Cambridge CoC;
- An improved and accurate understanding of the problems, issues, and needs of persons experiencing homelessness and at-risk populations;
- Produce an unduplicated count of persons experiencing homelessness in the CoC; and
- Increased information sharing with funders, boards, and other stakeholders to help inform meaningful system design and policy decisions.

Cambridge's HMIS Software

The CoC selected Clarity Human Services ("Clarity") a web based HMIS software owned by Bitfocus, Inc., ("Bitfocus") to be the HMIS software solution. It empowers human services providers, agencies, and communities to manage real-time client and services data. The City's Department of Human Service Programs contracts directly with Bitfocus, Inc. for this software and supports end-users with help desk, ongoing training, and project customization.

Clarity features:

- Combines the ease of the internet and the performance of a powerful database
- Protects client confidentiality by carefully restricting access
- Has robust client and referral tracking, case management, agency and project indexing
- Has an advanced reporting tool to understand and use key data
- Facilitates the secure sharing of data to help providers to effectively and efficiently perform client case management
- Ensures client, project, and agency-level data is available and accessible to all Partner Agencies in accordance with Federal, State, and local data sharing policies
- User-friendly, requiring a minimum learning curve for data entry and generation of reports
- Ensures project and agency-wide reports are easily produced by agencies

1. ROLES AND RESPONSIBILITIES

The roles and responsibilities of each group identified below are not meant to be all inclusive and a successful HMIS implementation requires all named groups and HMIS agencies to work together. Some roles and responsibilities may overlap between groups.

Policy: The Planning and Development Office (P&D) of the City of Cambridge Department of Human Service Programs is responsible for system administration and project management of the Cambridge HMIS.

Procedure: P&D will act as the Lead Agency for the Cambridge HMIS. P&D will help agencies to gain access to the database system, as well as provide training and technical assistance to the Partner Agency staff.

1.1 HMIS Lead Agency Responsibilities

As HMIS Lead for the Cambridge CoC the HMIS System Administrator:

a. Oversees the HMIS project and has primary responsibility for all HMIS activities.
b. Ensures HMIS compliance with all HUD rules and regulations.
c. Establishes and facilitates the HMIS Working Group.
d. Attends, provides information to and assists in facilitation of the CoC (HSPC) meetings.
e. Encourages and facilitates participation in the HMIS from homeless service provider agencies within the geographic area of the CoC.

f. Makes public all applicable HMIS Working Group meetings, inviting participation from the HMIS community at large.
g. Consults with the CoC to develop HMIS policies and procedures in compliance with HUD regulations and facilitates at least an annual review and approval from the HMIS Working Group.
h. Subject to oversight of the HMIS Working Group, negotiates, approves and executes annual contract with HMIS vendor.
i. Provides HMIS User training to all new users and refresher trainings as needed.
j. Develops and maintains remote accessible training materials for all HMIS users.
k. Creates HMIS User accounts and control access to HMIS.
l. Communicates all system-wide changes to Agency Administrators via direct emails, announcements on cambridgecoc.org and/or in quarterly Working Group and CoC meetings.
m. Provides technical support to Agency Administrators and End Users.
n. Serves as intermediary between Partner Agencies and the HMIS vendor.
    I. Completes software testing as needed.
    II. Submits tickets on behalf of Partner Agencies when Cambridge HMIS Staff is not able to solve a technical issue.
    III. Informs all HMIS Users of any planned or unplanned service outages via direct email or announcement on login page of cambridge.clarityhs.com
o. Establishes project setup and onboarding for newly participating agencies.
p. Responds to Partner Agency requests for customization of data collection for additional elements beyond those required by the most current published version of the HMIS Data Standards.
q. Builds, runs and makes available custom reports specific to projects/agencies to help monitor data quality and/or progress toward performance goals.
r. Responsible for design, technical oversight and local and HUD reporting for the Cambridge Coordinated Entry project (C-CAN).
s. Operates a Data Quality Improvement Program.
    I. Understands the data quality elements to be submitted with the SPM, APR and CAPER and ESG-CV report.
    II. Systematically monitors the data.
    III. Communicates regularly with the CoC and individual providers to ensure stakeholders are informed and have the resources to address data quality concerns.

s. Oversees participation in Rehousing Data Collective, the statewide data warehouse administered and operated by the Department of Housing and Community Development (DHCD).
    I. Completes quarterly data uploads to DHCD portal
    II. Oversight of user access and accounts within the Cambridge CoC
    III. Runs reports from RDC data set

1.2 Partner Agency/Covered Homeless Organization (CHO) Responsibilities

Definition: Any organization (including all its affiliates) that records or uses or processes Personally Identifiable Information (PII) from clients experiencing homelessness or those at risk of experiencing homelessness for an HMIS (Section 4.1.1, 2004 HMIS Data and Technical Standards).

Policy: Any agency participating in the Cambridge HMIS will abide by all policies and procedures outlined in this manual.

Procedure: Any agency, organization or group who has signed an HMIS Partner Agency Agreement with DHSP will be given access to the Cambridge HMIS through trained HMIS End Users.

Policy: The Executive Director of each Partner Agency within the Cambridge CoC participating in the Cambridge HMIS shall follow, comply and enforce the HMIS Partner Agency Agreement.

Procedure: A completed original, scanned, or digitally signed HMIS Partner Agency Agreement must be submitted to the HMIS Lead Agency before program implementation or user training on the Cambridge HMIS. The HMIS System Administrator will upload the agreement to the Agency files section of HMIS (Clarity).

Partner Agencies using the HMIS are key stakeholders in the success of the HMIS. All Partner Agencies will:

- Agree to abide by all policies and procedures outlined in this HMIS Policies and Procedures Manual
- Ensure that all employees and agents comply with the established policies and procedures
- Participate in monitoring and oversight procedures as conducted by the HMIS Lead on behalf of the CoC Board

- Ensure staffing, training, and secure equipment necessary to implement and ensure HMIS participation
- Ensure they meet the Privacy and Security requirements detailed in the HMIS Data and Technical Standards.

1.3 Partner Agency Administrator

Policy: Each Partner Agency will play a leadership role in the successful implementation of the HMIS within their agency and projects. To achieve this, Partner Agencies will identify an HMIS Agency Administrator (primary point person).

Procedure: Each Partner Agency shall designate at least one Agency Administrator, a representative that attends the HMIS Working Group meetings and who can effectively communicate information to and implement new procedures with the rest of their agency. While the HMIS Lead will attempt to document communication for circulation amongst partners, it is the requirement of each participant to share the contents of the meeting with HMIS users at their agency.

Functioning as the main liaison with the HMIS Lead, Partner Agency Administrators (primary point persons) are responsible for:

- On-site and first level support to their end-users (where there are more than one)
- Project compliance with Policies & Procedures
- End User adherence to workstation security policies
- Detecting and responding to violations of the Policies & Procedures
- Data quality monitoring and reporting
- Resolving any data quality issues as quickly as possible
- Preparation and review of all data relevant to required HUD or City reporting
- Confirmation of PIT and HIC data and any notification to HMIS Lead of any changes to project inventories (new projects, change in bed inventory for existing projects, ending projects)
- Directing staff to be trained in HMIS to register for training at: https://cambridgecoc.org/training/
- Regular attendance and participation in HMIS Working Group meetings

1.4 Agency Staff (End Users)

Policy: Any individual working on behalf of the Partner Agency (employee, contractor, and volunteer) that collects information for HMIS purposes must be designated as an

HMIS End User, and therefore is responsible for adhering to the policies and procedures set forth in the manual. Anyone who collects any HMIS data (electronic or paper) or creates reports from the system is deemed an HMIS end user. HMIS End Users are held accountable for the custody of client level data and for the privacy, confidentiality, and security of that data. End Users must be aware of the sensitivity of client-level data and must take reasonable and appropriate measures to prevent its unauthorized disclosure. End Users are responsible for protecting institutional information to which they have access and for reporting security violations.

Procedure: End Users will complete required trainings and submit a signed User Responsibility Agreement and Code of Ethics (Appendix F) prior to obtaining access to HMIS. Directors, managers, or front-end staff that will not enter client level data but have a role in collection or oversight of it will complete the mandated Privacy and Security training and other HMIS training related to HMIS Data Elements.
End Users:

- Safeguard client privacy through awareness of and compliance with confidentiality policies
- Complete data collection as specified by training and other documentation
- Must be trained by Cambridge HMIS staff and sign an End User Agreement prior to receiving a login to the HMIS.
- End Users not logging into Clarity to enter HMIS data will receive Privacy and Security and HUD HMIS data collection trainings. The HMIS Lead will obtain their End User agreement and keep it on file.

1.5 HMIS Working Group

Policy: The Cambridge HMIS Working Group consists of Agency Administrators from the CoC's Partner Agencies and provides oversight and guidance to HMIS. The group is open to the HMIS community at large and reports back to the CoC Board on relevant matters.

Procedure: The HMIS Lead Agency sends communications to the HMIS Working Group via email regarding upcoming meetings, document review and approval, software changes, and HUD updates.
The Working Group has the following responsibilities:

- Coordinates with the HMIS Lead to guide the HMIS implementation
- Meets, at the minimum on a quarterly basis and are the discussion and decision-making group for Cambridge HMIS
- Advises the operations, policies, and procedures of the CoC HMIS implementation.
- Oversees and informs operation of the HMIS by the designated HMIS Lead as outlined in the HMIS Governance Charter and works to monitor performance targets as established by the CoC

- Is the main venue to educate Partner Agencies on HMIS policies and procedures, with the expectation for members to communicate this information to End Users

1.6 Non-Participating HMIS Partner Agency

Agencies using a different instance of HMIS that are not DV providers must provide DHSP access to their HMIS. Non-Participating HMIS Partner Agencies must assign a staff member to be the primary point of contact with HMIS Project Staff and submit regular data quality reports as outlined in the Data Quality Improvement Plan.

1.7 HMIS Participation Policy

Mandated Participation

All projects that are authorized under HUD's McKinney-Vento Act as amended by the HEARTH Act to provide homeless services must meet the minimum HMIS participation standards.[1] These participating agencies are required to comply with all applicable operating procedures and must agree to execute and comply with the community approved HMIS Agency Partner Agreement.

Voluntary Participation

Non-funded partners providing services to people experiencing or at risk of homelessness cannot be required to participate in HMIS by the local community. However, the CoC and HMIS Leads work closely with non-HUD funded partners to articulate the benefits of the HMIS and to strongly encourage their participation. In addition to the benefits that HMIS will bring the non-required agency, adding this data to the HMIS provides more comprehensive client data to document their homelessness, more accurately illustrates the scope of homelessness in the community, establishes greater coordination among providers, and keeps the CoC competitive in federal funding allocation processes. The benefits and goals expected of CoCs relative to HMIS participation are put forth in HUD's Data TA Strategy to Improve Data and Performance.

2. IMPLEMENTATION POLICIES AND PROCEDURES

2.1 Data Collection Requirements

Data collection in HMIS primarily focuses on individuals or households who are homeless or at risk of becoming homeless. It is important for agencies, especially emergency services providers,

to know basic information about clients they serve, their household composition and the services they received. HMIS is a benefit to agencies using it because it allows them the ability to create reports that show meaningful information on the populations they served, including services provided and outcomes across time.

Policy: HUD's minimum standards require that individuals or families who are homeless or at risk of becoming homeless and are accessing services from an agency be engaged for HMIS data collection. Details on data collection and data elements can be accessed here: https://files.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf

Real time data entry is encouraged and considered to be best practice. In a system where data from Partner Agencies is interconnected in service of coordination and tracking outcomes, timeliness is one of the most important aspects of the HMIS. HUD has included this in their SNAPS document on Data TA Strategy to Improve Data and Performance, citing that well performing CoCs will have projects directly entering data within two hours for crisis response and project starts and exits, and that PSH projects will enter all data withing 24 hours. However, in cases where real time cannot be accomplished the procedure and timeframes put forth in the Cambridge HMIS Data Quality Improvement Plan are required to be followed.

Procedure: Staff should conduct the intake process with new clients, establishing they are eligible for services, and proceeding with the consent process outlined in the help documentation found on cambridgecoc.org/hmis.

Clients can choose to not participate in HMIS, or to participate but not share their information with other Partner Agencies. In the case of the former, End Users must still enter a record, but they will do so without any PII. In the case of the latter, End Users will create a record and mark it as "Private" in Clarity, thus locking the record and preventing other Partner Agencies from finding it in a search. The software also allows for locking specific program enrollments, when applicable.

If a project serves families, information must be collected on each family member, not just the head of household.

2.2 Technical and Security Standards

Policy: Partner Agencies must meet the technical standards outlined below to participate in the Cambridge HMIS.

Procedure: The Clarity Human Services software takes advantage of the latest in web technologies. For both security and compatibility, a Partner Agency's local IT Staff should ensure all workstations are outfitted with the latest version of the web browser staff use.

The following web browsers are supported by Clarity:
Firefox, Explorer, Safari, Chrome, Microsoft Edge

Connection to the internet is the sole responsibility of the Partner Agencies and is a requirement to participate in the Cambridge HMIS.

All Operating systems should have the latest Service Pack applied. Network design should allow for uninterrupted communication between Application, Database, Report, and Batch servers. Communication should be capable using the following standard protocols TCP/IP, WIN DNS, Named Pipes, and NetBIOS. All communication between servers should be designed to be performed on Local Area Network.
For security purposes, all computers must have the following:

- An updated and adequate firewall protection
- Virus protection software in which virus definition must be updated regularly

2.3 Maintenance of Computer Equipment/Data Access Location

Policy: Partner Agencies will commit to a reasonable program of equipment maintenance to sustain an efficient level of system operation. All security standards should be enforced regardless of the location of the connecting computer.

Procedure: The Partner Agency will be responsible for the maintenance

- Purchase of and upgrades to all existing and new computer equipment for utilization in the system
- All workstations must be password protected with the “screen timeout” setting or equivalent enabled and they may not be located where screens are visible to non-authorized persons.
- Workstations used off-site, including laptop and other mobile devices, should have appropriate and current firewall and virus protection.

2.4 HMIS Technical Support Protocol

Policy: The HMIS Lead Agency will provide technical support to all Partner Agencies as needed on the use of the HMIS/Clarity Human Services software.

Procedure:

1. End Users should direct technical questions to their Agency Administrator.
2. If that person is unavailable and/or after consultation with said person, the question is still unresolved, direct the question to the HMIS Lead who will determine the appropriate

procedure to be followed. Send an email to **mcolangelo@cambridgema.gov** or call 617-349-6966.

HMIS technical support staff:

- Is available for HMIS Support on Monday from 8:30 AM to 8 PM, Tuesday through Thursday, from 8:30 AM to 5PM and Friday, 8:30 AM to 12 PM.
- Strives to answer all technical support tickets within two (2) business days, but workload, holidays, and availability of staff may delay response.

After the normal business hours of the Cambridge HMIS Lead/Planning and Development office:

- Research on-line help and/or training materials by going to the Clarity Human Services Help Site.

2.5 Participation Fees

Policy: The Cambridge CoC reserves the right to charge a participation fee for Partner Agencies to use the system, as well as User License fees.

Procedure: Costs of user licenses are currently covered by the CoC and HMIS Leads, through grant funds. There is a cap of user licenses per agency, which varies, depending on the number of users in the system overall within a given contract year. Partner Agencies requesting licenses beyond the allotted amount may be charged a participation fee.

2.6 Computer Equipment and Supplies

Policy: The Cambridge CoC may provide computer equipment and supplies to a Partner Agency at the HMIS Lead Agency's discretion.

Procedure: Any inquiries about computer equipment or supplies related to the functioning of HMIS should be made by contacting the HMIS System Administrator.

3. SECURITY POLICIES AND PROCEDURES

3.1 User Authentication

Policy: Cambridge HMIS can only be accessed with a valid username and password combination. The HMIS Lead will provide unique username and initial password for eligible individuals after

completion of required training and signing of the User Policy, Responsibility Statement and Code of Ethics and receipt of these Policies and Procedures.

Procedure:

- The Partner Agency will determine which of their employees will have access to the Cambridge HMIS. User access will be granted only to those individuals whose job functions require access to the system.

- Proposed User must complete the required training and demonstrate proficiency in use of the system

- Proposed User must sign the User Policy, Responsibility Statement and Code of Ethics stating that they have received training, will abide by the Policies and Procedures, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in the system relevant to the delivery of services to people.

- HMIS System Administrator will be responsible for the distribution, collection, and storage of the signed User Policy, Responsibility Statement and Code of Ethics Statements which certifies receipt of these Policies and Procedures.

- The HMIS System Administrator will assign new user with a username and an initial password.

- Sharing of usernames and passwords will be considered a breach of the HMIS User Agreement as it compromises the security to clients.

- The Agency Administrator is required to notify the HMIS System Administrator immediately when an End User leaves employment with the organization or no longer needs access.

- HMIS System Administrator will terminate access upon notification of the Agency Administrator within 1 week of receiving notification of End User's departure.

3.2 Passwords

Policy: User will have access to the Cambridge HMIS via a username and password. Passwords will be reset every 180 days. User will maintain passwords confidential.

Procedure:

- The HMIS Administrator will provide a new End User a unique username and temporary password after required training is completed.
- End User will be required to create a permanent password that is between eight and sixteen characters in length.

- It must also contain characters from the following four categories:

  (1) uppercase characters (A through Z),
  (2) lower case characters (a through z),
  (3) numbers (0 through 9), and
  (4) non-alphabetic characters (for example, $, #, %).

- For security purposes, the Forced Password Change (FPC) will occur every 180 consecutive days and the End User will be prompted to enter a new password. Users may not use the same password consecutively but may use the same password more than once.
- After 60 minutes of inactivity, End User will get a session timeout warning popup that will allow End Users to continue their session or will automatically log the user off after 60 minutes of inactivity.
- End User can reset their own password from the log-in screen.
- Access permission will be revoked after the End User unsuccessfully attempts to log on three times. The End User will be unable to gain access until they reset their password or after one hour.

3.3 Extracted Data

Policy: All HMIS Users are required to ensure that client identifying information is never sent across an unencrypted network, saved in an unprotected folder on a computer, or, in the case of hard copies of client identifying information, stored anywhere other than a locked file cabinet or office.

Procedure:

- Client Identifying Information cannot be sent over unsecured email either between a Partner Agency and CoC and HMIS staff at DHSP or between staff at a Partner Agency.
- The only permissible way to discuss an individual client over email is using the client's ID number or through use of a secure email encryption software system.
- The staff messaging system in Clarity Human Services is a secure alternative for sharing client information.

3.4 Hardware Security Measures

Policy: All computers and networks used to access Cambridge HMIS must have virus protection software and firewall installed. Virus definitions and firewall must be regularly updated.

Procedure: A Partner Agency must regularly update virus definitions from the virus software vendor. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is accessed.

Policy: A Partner Agency must protect systems they use to access HMIS from malicious intrusion behind a secure firewall. It may also commit itself to additional security measures beyond this standard if in line with HMIS regulations.

Procedure: Each Partner Agency must maintain its own up to date firewall, however, each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization.

3.5 Backup and Recovery Procedures

The HMIS vendor stores client information and all other HMIS data in an encrypted centralized database, with daily and weekly backup procedures. Bitfocus employs information security and risk prevention practices that meet or exceed the minimum standards required by HUD, the State of Massachusetts, and the City of Cambridge. All client-level data in the Cambridge HMIS is hosted in secure, US-based facilities regularly evaluated for security and privacy best practices. At a minimum, data center facilities maintain current, independent audits certifying compliance with the following industry standards:

- SOC 2 Type II
- HI-TRUST

3.6 Security Review

Policy: The HMIS Lead Agency will complete an annual security review to ensure the implementation of the security requirements for itself and Partner Agencies.

Procedure: The HMIS Lead Agency will conduct a security review that includes the completion of a security checklist ensuring that each security standard is implemented.

3.7 Security Violations and Sanctions

Policy: Any User found to be in violation of security protocols of the organization procedures or Policies and Procedures will be sanctioned accordingly. All Users must report potential violations of any security protocols described in the Policies and Procedures.

Procedure:

- Users are obligated to report suspected instances of noncompliance and/or security violations to the Agency Administrator or HMIS System Administrator as soon as possible.
- The Agency Administrator or HMIS System Administrator will investigate potential violations.
- Any User found to be in violation of security protocols will be sanctioned accordingly. Sanction may include but are not limited to suspension of system privileges and revocation of system privileges.

More detailed Policies and Procedures for responding to security breaches and other security incidents are outlined in section 5 of this document.

4. OPERATIONAL POLICIES AND PROCEDURES

4.1 Training

User Training

Policy: All HMIS End Users must complete all beginner user training prior to gaining access to Cambridge HMIS. All End Users must complete an annual Privacy and Security Training and renew their User Responsibility agreements in order to maintain access to the HMIS.

Procedure:

- The Partner Agency Administrator or Executive Director will refer new staff for HMIS training by directing staff to register at cambridgecoc.org/training.
- The HMIS Lead is responsible for development and distribution of End User aids, reference material, and other supports, including workflow documentation available from Bitfocus.
- All training content will be accessed via cambridgecoc.org/hmis/training-guides-and-manuals.
- The HMIS Lead will provide HMIS application training in both in-person and remote format.

- End Users must successfully complete the required HMIS Beginner Training to demonstrate proficiency in the system and understanding of the Policies and Procedures.
- Failure to complete annual Privacy and Security Training may result in a revocation of access to the Cambridge HMIS.
- If additional or specific training needs arise, the HMIS Lead may arrange for special training sessions. All Partner Agencies will be informed of trainings via email and the Cambridge CoC website.

Report Generation Training

Each Partner Agency is strongly encouraged to request its Agency Administrator to review training resources on how to develop Partner Agency-specific reports using the HMIS reporting application that is a part of the HMIS solution. The HMIS Lead will provide recorded training and related documentation from Bitfocus.

4.1 Consent to Share Information and Confidentiality

Policy: Each Partner Agency must ensure that their clients complete a HMIS/C-CAN Client Consent Form in order for their PII to be shared with other agencies participating in HMIS. If the client refuses to provide consent, only the agency serving the client will have access to their information. Clients cannot be denied services for refusing to provide consent. A copy of the form will be provided to the client upon request.

Procedure

- Partner Agencies must post a Cambridge HMIS Privacy Statement (Desk Sign) (Appendix A) that refers to and summarizes the content of the Notice of Privacy Policy wherever client intake meetings occur.
- Partner Agencies must have available and provide a copy of the Notice of Privacy Policy (Appendix B) upon request.
- Client consent in Cambridge HMIS is universal; therefore all End Users will search Clarity before engaging the client in the consent process, in order to determine if this has already taken place at another Partner Agency or with their Agency during a time frame where the consent is still valid.
- End Users will notify the client that the information they collect will be entered into HMIS and will explain the purposes of sharing data across Partner Agencies.
- The client will be provided the CHMIS/C-CAN Client Consent Form (Appendix C) for review, will be explained its content and will be asked to sign, date, and print their name on it if they consent. (If this is done electronically, they will only need to sign their name.)

- Clients that provide permission to enter personal information allow for Partner Agencies within the CoC to share client and household demographic data.
- If the client declines to share information with the Cambridge HMIS Partner Agencies, the End User must indicate their response in Clarity and upload a paper form to the Client's file section.
- Clients who are actively fleeing a domestic violence situation should not be asked to consent to share their PII.
- The End User will record the client's response in Clarity, within the privacy screen for the respective client.
- Partner Agencies will store signed consent forms the client's Clarity record, including forms the client did not sign, but are signed by the End User, certifying that the client was informed of HMIS data collection and their rights.
- If a client refuses to provide consent, the User should still create a client record, but they will set it to "Private" on the client privacy page in Clarity.
- If a client refuses to provide consent to share their information in HMIS, the End User completing the consent process will sign the form in order to show that the consent process was conducted.
- If a client refuses to participate or be identified in HMIS, the User should not include any personal identifiers (such as first name, last name, social security number, date of birth, etc.) in the client record. Instead, User should include a client identifier to recognize the record in the system.
- If a client consents to share information after previously denying consent, End Users must follow the same procedures that were specified above involving the completion of the initial consent form.

Policy: All standards described in this manual pertain to any homeless assistance organization that records, uses or processes personally identifying information (PII) for the Cambridge CoC's HMIS. One exception exists to this policy: any Partner Agency covered under HIPAA is not required to comply with the standards in this manual if the Partner Agency determines that a substantial portion of its PII about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules (Section 4.1.2, 2004 HMIS Data and Technical Standards).

Procedure: A Partner Agency must comply with HIPAA rules instead of HMIS policies if it determines that a substantial portion of its PII about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules. Exempting HIPAA covered entities from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules.

4.2 Revocation of Consent

Policy: In the event that a client previously gave consent to share their PII in the Cambridge HMIS and chooses at a later date to revoke consent, a Revocation of Consent form (Appendix E) must be completed and signed by the client.

Procedure

- Upon request, the Partner Agency must ensure that Revocation of Consent is received by the HMIS Lead. The HMIS System Administrator will then modify the client information by removing any personal identifiers (First Name, Last Name, Social Security Number, and Date of Birth from the client record.
- End Users should communicate with HMIS Lead by including a client identifier to recognize the record in the system.
- End Users should never overwrite PII based on a revocation. The HMIS System Administrator will complete this task and notify any other Partner Agency that is also currently serving the client.
- Partner Agencies that have previously provided services will still have access to client protected personal information.

4.3 Verbal Consent for Services

Policy: Due to the COVID-19 public health emergency and to more efficiently serve clients, the HMIS Lead Agency may authorize the use of a verbal process for assessment and documentation, when no other consent is present. The verbal process does not replace in person enrollment. This policy shall be re-evaluated at the beginning of 2021.

Procedure:

- The HMIS Lead Agency must provide written authorization to Participating Agencies wishing to use the verbal consent process.
- The use of verbal consent will only be necessary when there is not a current HMIS Consent form (ROI) in place for the client.
- The verbal process to collect information shall replace a written signature on the Cambridge, MA HMIS and Cambridge Coordinated Access Network (C-CAN)

Client Consent Form with a telephonic signature which will allow for authorized access to the client's data, and shall collect relevant identifiers to ensure unique identification of the individual and record of the consent.

- Authorized Partner Agencies shall certify in the HMIS they have talked to the individual, and to the best of their ability, collected the required unique identifiers and have indicated such by including a telephone reference number on the electronic file in the HMIS.
- Verbal Consent process shall be monitored on an ongoing basis and should be used sparingly when a written signature is not possible.
- End Users at approved agencies will follow this procedure to ensure proper steps are taken to protect client PII and ensure privacy protections are observed:

  Agency staff will identify if a client already has a valid consent in HMIS.

  - If they do, agency staff will continue using standard procedures.
  - If there is no valid consent, or if the client is not in the HMIS, agency staff will perform the following actions:

  In lieu of reviewing the HMIS Client Consent to Release Information (ROI), you will need to state the following to the client when obtaining verbal consent:

  - *"Before I proceed, I need to explain that I will be entering your information into the computerized Homeless Management Information System or HMIS. The information you provide will be shared with other partner agencies that may be able to assist you. Also, it is my responsibility to make sure you are aware of how your information may be used and your rights to privacy. You can find a copy of the HMIS Privacy Policy at cambridgecoc.org/policies-and-procedures/ or I can send it to you via email or text. May I have your consent to share the information you provide?"*
  - If verbal permission is granted, agency staff will note it in the appropriate location in HMIS record, then continue using standard procedures.

4.4 Data Sharing

Policy: Data sharing among Partner Agencies happens when a client agrees to have their information shared.

Procedure: Projects have the opportunity to share client level data. Data sharing is dependent on the Agency's participation and the client's authorization. No client information is shared in Cambridge HMIS until the Partner Agency enters the ROI indicating a "Yes" of consent to share

information. Case notes entered by one agency are not viewable to End Users at another Partner Agency.

4.5 Client Record Access and Correction

Policy: The Partner Agency must allow a client to inspect and to have a copy of any PII about the client stored in HMIS and offer to explain information that the client may not understand.

The Partner Agency must consider any request by a client for correction of inaccurate or incomplete PII pertaining to that client. A Partner Agency is not required to remove any information but may, alternatively, mark information as inaccurate or incomplete and supplement it with additional information such as an indicator of data quality. A Partner Agency can reject repeated or harassing requests for access or correction (Section 4.2.5, 2004 HMIS Data and Technical Standards).

Procedure: A client will provide a signed written request to a case manager to see the client's own record. The case manager will forward the request to the Agency Administrator who will verify the client's identity. The Agency Administrator will contact the HMIS System Administrator to consult on best practice to comply with this request.

4.6 Client Grievance

Policy: Clients have a right to file a grievance with a Partner Agency or with the HMIS Lead Agency. Partner Agencies must have written grievance procedures that can be provided to a client upon request. Any unresolved grievances may be brought the HMIS Lead Agency. Clients will not be retaliated against for filing a complaint.

Procedure:

- Clients will submit grievance in writing directly to Partner Agency with which they have a grievance.
- Upon client request, the Partner Agency will provide a copy of their grievance procedure and the Cambridge HMIS Policies and Procedures Manual.
- Partner Agency will send written notice to the HMIS System Administrator when there is any HMIS related grievance. The HMIS System Administrator will maintain a record of all grievances.
- If a client is not satisfied with the results of the grievance with the Partner Agency, the client may complete a Cambridge HMIS Grievance Form (Appendix D).

5. DATA POLICIES AND PROCEDURES

5.1 Data Quality

HMIS users are required to ensure the quality of the information that they enter into HMIS, as stated in the User Policy, Responsibility Statement and Code of Ethics and the Data Quality Improvement Plan. There are several reasons why data quality is important to everyone, from clients to users to agencies -- to the CoC as a whole. If information is not collected accurately, clients may experience issues trying to coordinate multiple service providers, receiving appropriate referrals, and determining their eligibility for services. HMIS users may have trouble helping clients appropriately without timely and accurate information being collected. Our CoC will face reporting and decision-making challenges without accurate data.

Policy: Cambridge CoC HMIS End Users will be responsible for the timeliness and accuracy of their data entry. The Partner Agency must maintain standards of regularly checking for data completeness, accuracy and timeliness.

Procedure: The Cambridge HMIS operates a regular schedule of data quality reporting for Partner Agencies, as described in the Cambridge HMIS Data Quality Improvement Plan. Street Outreach and Night by Night Emergency shelters must submit these reports monthly, all other project types submit quarterly. The Cambridge HMIS Data Coordinator oversees and administers all tasks pertaining to this operation.

5.2 Data Use and Disclosure

Policy: All Users will follow the data use Policies and Procedures to guide the data use of client information stored in the Cambridge HMIS.

Definitions: Client data may be used or disclosed for system administration, technical support, program compliance, analytical use, and other purposes as required by law, and as outlined by the Privacy Notice, HMIS Partner Agency Agreement and HMIS User Policy, Responsibility Statement and Code of Ethics. Uses involve sharing parts of client information with persons within an organization. Disclosures involve sharing parts of client information with persons or organizations outside an organization.

Procedure:

- Partner Agencies may use and disclose data contained in the system to support the delivery of services to clients experiencing homelessness or at-risk of homelessness in Cambridge, MA.

- Each of the Partner Agencies shall have access to their respective client data stored in the system. The Cambridge HMIS will use the data for various purposes including administrative functions, technical support, program compliance, and analytical use. Unless restricted by other laws, the information collected can be shared and disclosed under the circumstances outlined in the Privacy Notice. Upon signing the client consent form, PII may be disclosed for service provision purposes.

5.3 Data Release

Policy: All Cambridge HMIS stakeholders will follow the data release Policies and Procedures to guide the data release of client information stored in the Cambridge HMIS.

Definition: Data release refers to the dissemination of aggregate or anonymous client-level data for the purposes of system administration, technical support, program compliance, and analytical use.

Procedure:

- No identifiable client data will be released by Partner Agencies to any person, agency, or organization for any purpose without written permission from the client.
- Each Partner Agency owns all data that is stored in the system. The Agency may not release personal identifiable client data without written permission from the client. Organizations may release program and/or aggregate level or de-identified data for all clients to whom the organization provided services.
- Each of the Partner Agencies may release aggregate or de-identified data about its own agency and projects. Aggregate or de-identified data may be released without organization permission at the discretion of the Continuum. The Cambridge HMIS may develop an annual release of aggregate data in a summary report format.

6. INCIDENT RESPONSE POLICIES AND PROCEDURES

Policy: To protect the data in the Cambridge HMIS and the integrity of the community level database, procedures have been put in place to ensure consistent responses to incidents (such as security breaches and/or inappropriate User, project, or agency actions). This plan, while subject to revision, is intended to address how the Cambridge HMIS and CoC will respond to any incident, including: assessing the incident, minimizing damage, ensuring rapid response, and documenting and preserving evidence.

An incident is any one or more of the following:

- Loss of information confidentiality
- Compromise of information integrity
- Theft or loss of physical IT asset, including computers, storage devices, printers, etc.
- Misuse of information, tools, etc. including but not limited to unauthorized transfer of client data, breaches of security or confidentiality.
- Sharing login information
- Infection of systems by unauthorized or hostile software
- An attempt at unauthorized access
- Unauthorized changes to organizational hardware, software, or configuration
- Reports of unusual system behavior

Procedure: The HMIS Lead will use the following guidelines when addressing a given incident in relation to HMIS.

Discover

Typically, an incident will come to the attention of the HMIS Lead when someone discovers something "not right" or suspicious. It may be discovered by the HMIS Lead or a variety of others involved in the implementation of the HMIS, including but not limited to: HMIS End Users, monitoring team, management staff, agency IT staff, a firewall administrator or an intrusion detection system.

Assess and Document

Actions will be taken to determine the following:

- Whether the incident is still in progress or is over.
- Scope of the issue, including how many records were affected and how many HMIS users were involved.
- The data or property that is threatened and how critical is it.
- The system or systems that are and/or were targeted, where they are located physically and/or on the network.
- Whether the incident is inside the trusted network.
- Whether the incident was intentional or accidental.
- Whether the situation resulted from an End User acting on their own, under the direction of a supervisor, and/or due to a general culture of the project or Agency.

Determine Response and Minimize Damage

In order to minimize risk and respond quickly, the HMIS Lead may act initially on its own to determine the appropriate response strategy and inform additional parties after the incident is contained. In determining the strategy, the following questions will be considered, and an incident level will be assigned.

- What is the scope and nature of the incident?
- Is an urgent response required?
- Can the incident be quickly contained?
- Will the response appropriately alert those involved in the incident?

Incident Level System (ranked from most severe to least)

Category 1 - A threat to HMIS security at a community-wide level
Category 2 - A threat to shared HMIS data elements
Category 3 - A threat to HMIS security within a Partner Agency or across shared projects
Category 4 - A threat limited to the scope of actions of one user

Responses: The following guidelines have been established to help guide the initial response. This list is subject to change based on the specifics of each incident that is encountered.

Isolate and contain the incident

- Incident level category 1 and 2 – This may result in temporarily disabling a particular feature, field option, or data sharing protocol.
- Incident level Category 3 and 4 – This may result in temporarily disabling access for a Partner Agency, project, or specific User.

Notify the following parties, as applicable depending on the category level of incident:

- Agency Executive Director (or equivalent), project managers, and specific End Users involved
- CoC Board
- All HMIS users

Initiate determination of Action Plan to address the incident.

Address the Incident

The HMIS Lead will work with the those involved to quickly resolve the issue. If, due to the severity of the risk, time does not allow the HMIS Lead to convene all parties prior to additional intervention, the HMIS Lead will convene such a group as soon as practicable following initial intervention in order to discuss an appropriate action plan to resolve the incident. This is intended to ensure all viewpoints are addressed and considered as part of the action plan. As appropriate and/or necessary, the HMIS Working Group and/or the CoC Board may also convene to ensure agreement on the action plan.

Establish an Action Plan

Once the incident is contained, the HMIS Lead will initiate the process of determining an Action Plan for moving forward. The Action Plan may include:

Partner Agency leadership and the HMIS Lead addressing the actions of staff and determining if additional action against the user is appropriate.

Partner Agency leadership establishing or modifying internal policies around HMIS usage and ensuring staff are properly notified.

Restoring Access – In cases in which the severity of the security risk resulted in revocation of access to the system, the HMIS Lead will, if appropriate, restore access once the Action Plan is established and corrective steps have been taken.

Terminating Specific User Access:

In severe cases, the HMIS Lead may, without warning to the End User, choose to ban the user from future access to HMIS.

This includes but is not limited to cases where a trained End User has knowingly and intentionally shared their personal password and login.

The HMIS Lead will inform the user's supervisor and the Agency Administrator of the termination and any necessary remediation efforts required to be completed by the Partner Agency.

In other cases, the HMIS Lead will notify the user and supervisor of the issue as a warning, but if the End User commits the same or similar action again, the HMIS Lead may ban the End User from future access, temporarily suspend the Users' account, and/or require the User to complete additional training before turning their access back on.

Final Resolution

In a case in which the Partner Agency, the HMIS Lead, Working Group and/or CoC Board are unable to come to an agreement regarding an Action Plan to resolve the incident, the HMIS Lead

maintains the right to terminate system usage for any action that violates or compromises client confidentiality based on access to or use of the system. Any Partner Agency wishing to contest the termination may submit a grievance to the CoC Board for review.

Document the Incident

Detailed documentation of the incident and response will be maintained by HMIS Lead. Any documentation referencing client files will use the client's unique identifier from HMIS as the key reference code to the file stored in the HMIS.

Notification of Affected Parties

Notification of incidents is important as HMIS is a shared database. Beyond the notification step as part of any response, there may be times in which it is necessary and/or appropriate to notify other groups, such as the CoC Board and general HMIS users. When necessary and/or appropriate, the HMIS Lead may post a general warning or notice to all users on HMIS to alert them of the incident and response or provide a more detailed account of the incident, response, and resolution.

Review Response and Update Policies

After any incident, the HMIS Lead will plan and take preventative steps so that the possibility of a similar incident occurring again will be minimized and update these policies as needed. The following will be considered:

- Whether an additional policy could have prevented the intrusion.
- Whether the failure to follow a procedure or policy allowed the intrusion, then consider what could be changed to further ensure the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Is additional follow up necessary?
- Were the response procedures sufficiently detailed and do they cover the entire situation? Can the response procedures be improved?
- Should any security policies be updated?

7. COMMON HMIS TERMS AND ACRONYMS

Term	Acronym	Brief Definition
Agency Administrator Agreement		The document each Agency Administrator signs agreeing to perform the Agency Administrator responsibilities.
Agency Partner Agreement		The Agreement between all Partner Agencies and DHSP that specifies the rights and responsibilities of DHSP and Partner Agencies.
Agency Privacy Policy		Each Partner Agency must have a Privacy Policy that protects the privacy and confidentiality of their Clients.
Audit Trail		An auditing system within Clarity Human Services software that monitors, records and reports on what valid users of HMIS are doing within the database.
Authentication		The process by which users validate their identity. In Clarity this entails establishing a unique Username and Password for each user license.
Cambridge HMIS	CHMIS	The HMIS implementation for the Cambridge, MA Continuum of Care. CHMIS is operated by the Planning and Development Office of the City of Cambridge's Department of Human Service Programs.
Clarity Human Services		HMIS software developed by vendor Bitfocus, Inc. and the software solution used by the Cambridge CoC to fulfill HUD's HMIS requirements.
Comparable Database		A database used by a victim service provider that collects Client-level data over time and generates unduplicated aggregate reports based on the data, in accordance with HUD regulations.
Confidentiality		A Client's right to privacy of the personal information that is communicated in confidence to a case manager (or other agency staff) that is stored within the HMIS.

Term	Acronym	Brief Definition
Continuum of Care	CoC	The group organized to carry out the responsibilities of addressing and ending homelessness that is composed of representatives of organizations, including nonprofit homeless service providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve homeless and formerly homeless veterans, and homeless and formerly homeless persons to the extent these groups are represented within the geographic area and are available to participate.
Covered Homeless Organization	CHO	Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes protected personal information on clients for an HMIS. Synonymous with Partner Agency.
Encryption		Conversion of plain text into encrypted data by scrambling it using a secret code that masks the meaning of the data to any unauthorized viewer. Computers encrypt data by using algorithms or formulas. Encrypted data are not readable unless they are converted back into plain text via decryption.
End User		An individual working on behalf of the agency (employee, contractor, and volunteer) that will collect information for HMIS purposes must be designated as an HMIS end user, and therefore is responsible for adhering to the policies and procedures set forth in the manual. A person who collects HMIS data (electronic or paper) or creates reports from the system is deemed an HMIS end user. HMIS end users are held accountable for the custody of client level data and for the privacy, confidentiality, and security of that data.
Exempt Agency		Any agency that is explicitly exempt from entering data into the HMIS by federal regulations. This includes victim service providers.
Homeless Management Information System	HMIS	A data system that meets HUD's HMIS requirements and is used to measure homelessness and the effectiveness of related service delivery systems. The HMIS is also the

Term	Acronym	Brief Definition
		primary reporting tool for HUD homeless assistance program grants as well as other public streams of funding related to homelessness.
HMIS Lead Agency		An entity designated by the CoC in accordance with the regulations to operate the CoC's HMIS on its behalf. (DHSP/Planning & Development Office of the City of Cambridge)
HMIS Working Group		Continuum-based committee consisting of HMIS Agency Administrators, Agency System End Users who convene for the purpose of ensuring consistent, effective operation of the Cambridge HMIS.
HMIS User Agreement & Code of Ethics		The document each HMIS User signs agreeing to the HMIS standards of conduct and operating policies and procedures.
Housing Inventory Chart	HIC	HUD requires each CoC to annually submit a chart that lists all homeless residential programs (both HMIS and non-participating), specifying the type and number of beds/units available to homeless persons within the geographic area covered by the CoC. The HIC information is entered into the program description section in HMIS.
Housing Opportunities for Persons with AIDS	HOPWA	Federal program dedicated to the housing needs of people living with HIV/AIDS. Under this Program, HUD makes grants to local communities, States, and nonprofit organizations for projects that benefit low-income persons living with HIV/AIDS and their families.
Length of Stay	LOS	The number of days between the beginning of services and the end of services. It is calculated using entry and exit dates or shelter stay dates. The HMIS offer calculations for discrete stays as well as the total stays across multiple sheltering events.
Longitudinal Data Analysis	LSA	A report that provides the HMIS data used to complete the AHAR, or Annual Homeless Assessment Report, submitted to Congress annually and to the Stella Performance. The LSA includes detail about households' system use that will allow CoCs to understand lengths of

Term	Acronym	Brief Definition
		homelessness, exits to permanent housing, and returns to household type.
Partner		Organizations that participate in HMIS; also referred to as "Agency" or "CHO."
Personally Identifying Information	PII	A category of sensitive information that is associated with an individual. It should be accessed only on a strict need-to-know basis and handled and stored with care.
Point in Time Count	PIT	An annual count of sheltered and unsheltered homeless persons during the last week in January that is required by HUD for all CoCs.
Projects for Assistance in Transition from Homelessness	PATH	Federal program that funds community-based outreach, mental health and substance abuse referral/treatment, case management and other support services, as well as a limited set of housing services for adults who are homeless or at imminent risk of homelessness and have a serious mental illness.
Release of Information	ROI	A signed (paper or electronic) document giving informed Client consent for sharing Client data.
Stella Performance	Stella P	A strategy and analysis tool that helps the CoC understand how the system is performing and models what an optimized system would look like that fully addresses homelessness in the CoC geographic area. Stella P provides dynamic visuals of CoCs' Longitudinal Systems Analysis (LSA) data to show how households move through the homeless system, and to highlight outcome disparities. It looks at the system's past performance to see where the community can make future improvements. Raw, de-identified data from HMIS is used for Stella P analysis.

Term	Acronym	Brief Definition
System Performance Measures	SPM	7 measures defined by the HEARTH Act that provide a more complete picture of how well the community is preventing and ending homelessness.

APPENDIXES

Appendix A CHMIS Privacy Statement/Desk Sign

Appendix B CHMIS Notice of Privacy Policy

Appendix C CHMIS/C-CAN Client Consent Form

Appendix D CHMIS Client Grievance Form

Appendix E CHMIS Revocation of Consent Form

Appendix F CHMIS User Responsibility and Code of Ethics

Coming Soon:

CHMIS Data Quality Improvement Plan (updated)

CHMIS Partner Agency Agreement (updated)

Appendix A

Cambridge Homeless Management Information System (HMIS)
PRIVACY STATEMENT

- We collect personal information directly from you for reasons that are discussed in our Privacy Notice.
- We may be required to collect some personal information by law or by organizations that give us money to operate this program.
- Other personal information that we collect may be used or disclosed to coordinate and improve services for persons experiencing homelessness, and to better understand the needs of persons experiencing homelessness.
- We only collect information that we consider to be appropriate.
- You may request a copy of our Privacy Notice.
- We will not deny services to any eligible client who refuses to furnish the requested information, provided that such refusal does not prevent our Agency from establishing that client's eligibility for services.
- The policies in our notice may be amended at any time. These amendments may affect information obtained by this organization before the date of the change. Amendments regarding use or disclosure of personal information will apply to information (data) previously entered in HMIS, unless otherwise stated. All amendments to our Privacy Notice must be consistent with the requirements of the federal HMIS privacy standards.

Appendix B

HMIS Notice of Privacy Practices

Cambridge, MA CoC
Homeless Management Information System (HMIS)

THIS PRIVACY NOTICE EXPLAINS UNDER WHAT CIRCUMSTANCES WE MAY SHARE AND DISCLOSE YOUR INFORMATION FROM THE CAMBRIDGE HMIS. THIS NOTICE ALSO EXPLAINS YOUR RIGHTS REGARDING YOUR CONFIDENTIAL INFORMATION.

PLEASE READ IT CAREFULLY.

If you have any questions about this Notice, you may contact either your service provider, or:

Cambridge Continuum of Care
51 Inman Street, Cambridge, MA 02139
617-349-6206
PlanningDev@cambridgema.gov

This Notice describes standards for the privacy of personal information collected and stored in the Cambridge Continuum of Care ("CoC") Homeless Management Information System ("HMIS"), as well as personal information collected for the purposes of the Cambridge Continuum of Care Coordinated Entry System (Cambridge Coordinated Access Network ("C-CAN)").

We ask for your permission to share confidential personal information that we collect about you (and members of your household, if applicable) with other providers using the same system. This confidential information is referred to as Personally Identifiable Information (“PII”). We are required to protect the privacy of your PII by complying with the privacy practices described in this Privacy Notice.

THE TYPE OF INFORMATION WE COLLECT IN HMIS

We collect and share both PII and general information obtained during your intake and assessment, which may include but is not limited to:

- Name and contact information
- Social security number
- Birthdate
- Demographic information such as gender and race/ethnicity
- History of homelessness and housing (including current housing status and where and when services have been accessed)
- Self-reported medical history including any mental health and substance abuse issues
- Case notes and services
- Case manager’s contact information

- Income sources and amounts; and non-cash benefits
- Veteran status
- Disability status
- Household composition
- Emergency contact information
- Domestic violence history
- Photo (optional)
- Uploaded documents pertaining to housing applications and placement eligibility

HOW YOUR PERSONAL INFORMATION IS PROTECTED IN HMIS

Your information is protected by passwords and encryption technology. Each HMIS user and participating organization must sign an agreement to maintain the security and privacy of your information. Each HMIS user or participating organization that violates the agreement may have access rights terminated and may be subject to further penalties.

HOW WE MAY USE AND DISCLOSE YOUR INFORMATION

For Housing: We create a record of your information including housing services you receive at our partner agencies. We need this record to provide you with quality services and to comply with certain legal requirements. Your service provider may use or disclose your information to other personnel who are involved in providing services for you. For example, a housing navigator may need to know disability information to provide appropriate housing resources. We also may use and disclose your information to people outside this agency who may be involved in your service coordination when you access services from our partner agencies.

For Streamlined Service Provision: We may use or disclose basic information about you so that you do not have to provide information more than once. This sharing, only when you access one of the participating agencies, can help avoid duplication of services and referrals that you are already receiving.

For Administrative Operations: We may use and disclose information for functions related to payment or reimbursement for services and to carry out functions including but not limited to legal, audit, personnel, oversight and management functions.

USES AND DISCLOSURES THAT DO NOT REQUIRE YOUR AUTHORIZATION

Data Retrieval: Cambridge HMIS will generate reports required by HUD, the CoC and other stakeholders. This will be at the level that does not identify individuals but can provide statistical data. The HMIS Lead Agency staff has access to retrieve all data in the Cambridge HMIS. The HMIS Lead Agency will protect client confidentiality in all reporting. Partner Agencies may also retrieve HMIS data entered to produce statistical reports including number of clients served for internal purposes, grant applications and other required reports, within the parameters of their own agency's program enrollments and services.

Data Transfer: The Cambridge CoC participates in the Rehousing Data Collective (RDC), a statewide data warehouse operated by the Department of Housing & Community Development (DHCD). HMIS data including PII are exported from HMIS to the RDC in accordance with its agreement with DHCD. Records transmitted to the warehouse are locked and PII is visible only to the RDC System Administrator and authorized staff from the software vendor (Green River) for purposes of deduplicating and deidentifying records for statewide research and reporting. Individuals may authorize disclosure of their PII to assist in service coordination if they receive services in multiple communities, but PII cannot be shared by the warehouse administrators without an individual's permission documented by a separate signed *Authorization for Disclosure of Personal Information* that pertains only to this warehouse.

Academic Research or Evaluation Purposes: Under certain circumstances, we may use and disclose information about you for research purposes. Any research/evaluation on the nature and patterns of homelessness (at the CoC-wide level) that uses PII HMIS data will take place only on the basis of specific agreements between researchers and the Cambridge HMIS Lead. These agreements must be approved by the HMIS Working Group and the CoC Board and must reflect adequate standards for the protection of confidentiality of data.

As Required by Law: We will use and disclose information when required to do so by federal or state law or regulation.

To Avert a Serious Threat to Health or Safety: We may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:

(1) the CoC 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.

OTHER USES OF YOUR INFORMATION

Other uses and disclosures of your information not covered by this Notice or the laws that apply to us will be made only with your written authorization. If you provide us authorization to disclose your information, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your information for the reasons covered by the authorization, except that, we are unable to take back any disclosures we have already made when the authorization was in effect, and we are required to retain our records of the services that we provided to you.

YOUR RIGHTS TO YOUR INFORMATION IN HMIS

Right to Revoke your Consent for Sharing Information in the HMIS: You may revoke your consent at any time. Your revocation must be provided either in writing or by completing the Revocation of Consent form. Upon receipt of your revocation, we will remove your PII from the shared HMIS database and prevent further PII from being added. The PII that you previously authorized to be shared cannot be entirely removed from the HMIS database and will remain accessible to the limited number of organization(s) that provided you with direct services.

Right to a Paper Copy of This Notice: You may ask us for a paper copy of this Notice at any time. To obtain a paper copy of this Notice, ask any staff person. You may also obtain a copy of this Notice at our website at https://cambridgecoc.org/policies-and-procedures/.

Right to a List or Partner Agencies: A current list of participating organizations that have access to your HMIS data can be obtained by asking a staff person, or going to https://cambridgecoc.org/hmis-participating-agencies/.

Right to Inspect and Obtain Copies: You have the right to inspect and obtain a copy of Personally Identifying and Program Enrollment information for services we have provided to you.

Right to Request an Amendment: If you feel that your information in our records is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as we keep the information. To request an amendment, you must submit a request in writing to your service provider.

Right to File a Compliant if you have a Grievance: If you believe your privacy rights have been violated, you may send a written grievance to this organization. You will not be retaliated against for filing a grievance. If your grievance is not resolved to your satisfaction, you may send a written grievance appeal to the Cambridge Continuum of Care, Planning and Development Office, City of Cambridge, 51 Inman Street, Cambridge, MA 02139.

CHANGES TO THIS NOTICE

The policies in this notice may be amended at any time. These amendments may affect information obtained by this organization before the date of the change. Amendments regarding use or disclosure of PII will apply to information (data) previously entered in HMIS, unless otherwise stated. All amendments to this privacy notice must be consistent with the requirements of the federal HMIS privacy standards. This organization must keep permanent documentation of all privacy notice amendments.

Effective 11/01/2020 Revised 8/14/2020

Cambridge, MA HMIS and Cambridge Coordinated Access Network (C-CAN) Client Consent Form

What is the Cambridge HMIS and Cambridge CAN?

The Homeless Management Information System (HMIS) is a computerized data collection system designed to collect client information about the characteristics and service needs of individuals and households at risk of or experiencing homelessness. The information collected in HMIS will help us to analyze and improve service delivery, identify programs you are eligible for, better understand homelessness, and evaluate the effectiveness of our services. The Planning and Development Office of the Department of Human Services for the City of Cambridge is the HMIS Lead Agency as defined by HUD. Clarity Human Services is the HMIS application used by the Cambridge Continuum of Care (CoC). The Cambridge Coordinated Access Network (Cambridge CAN/C-CAN) is the coordinated homeless response system for the City of Cambridge, MA.

In Cambridge, all the agencies that participate in entering client data in HMIS share some of that data with each other if needed. This means that if you receive services from a program participating in the Cambridge HMIS and later need assistance in another program that also participates, staff at the second agency will search for your name and be able to find your profile. Then you will be asked to confirm your existing information in HMIS (like your name, date of birth and social security number). The second agency will be able to see what kind of services you've received in the past. If you are enrolling in C-CAN, staff you work with will be able to use your HMIS record to help provide documentation of your time experiencing homelessness.

If you would like to see a list of the agencies that participate in the Cambridge HMIS, please ask the agency you are receiving services from presently for a list of the Participating Agencies or visit cambridgecoc.org/hmis-participating-agencies/. Please note that the list of agencies contributing data to HMIS can change frequently and without notice, therefore the website should be referred to for the most current list.

Because Cambridge HMIS contains sensitive data, we take your privacy very seriously. The following protections for your data are in place:

- Individual client data is only viewable by certain qualified staff at each participating agency
- In order to participate in the Cambridge HMIS, leaders at each agency must sign a Partner Agency Agreement that includes a commitment to protecting client data and maintaining confidentiality.
- In order to use HMIS, agency staff must successfully complete trainings that inform them of how to protect client privacy.
- The Cambridge HMIS is hosted on a secure server and is data encrypted.

What information is collected in the HMIS database?

We collect Personal Identifying Information (PII) and general information obtained during your intake and assessment, which may include but is not limited to:

- Your name and your contact information and address
- Your social security number and date of birth
- Your basic demographic information such as gender, race and ethnicity
- Your veteran status
- Your photo (at select agencies only and is optional)
- Your history of homelessness and housing (including your current housing status, and where and when you have accessed services)
- Documents related to housing eligibility

If you are assessed for C-CAN, we also may share self-reported medical history and disability status, including mental and physical health concerns, substance abuse history, and HIV/AIDS status, income sources and amounts, and non-cash benefits, information about other members of your household and your self-reported history of domestic violence.

Why is this information collected?

- To provide and coordinate services
- To assess your needs and the needs of others in our community
- To reduce the duplication of information
- To reduce the amount of time you spend trying to get services and make sure you get the services you need
- To meet requirements of funders such as the U.S. Department of Housing and Urban Development (HUD)
- To develop and improve programs to work towards ending homelessness in our community

How is the information used?

- Based on your needs, social service and housing provider agencies may use HMIS to exchange, share and/or release information collected about you. The purpose of this form is to receive your permission to share this information as needed.
- This may include coordinating referrals for housing services and, if applicable, help in verifying instances of homelessness.
- Information may be used for research and evaluation. If so, your personal identity will never be a part of any research reports.

What are my rights?

- You have the right to receive services, even if you do not sign this consent form. Providers may not refuse to provide you with services if you refuse to sign, but they are still required to ask you questions for intake and enter that information into HMIS, however, they will either lock the

record (preventing it from being seen by other participating agency staff) or de-identify it so there is no way of determining your identity. If you are actively fleeing domestic violence, we are prohibited from entering any identifying data about you in HMIS. If you are assessed for C-CAN, your signature on this document will help us determine your eligibility for housing programs.

- If you have enrolled in C-CAN, you may stop your participation in that program at any time by contacting the C-CAN Coordinator at cambridgeCAN@cambridgema.gov or 617-349-7715.

- You have a right to see a copy of the information in your HMIS record and to ask for changes upon written request.

- You have a right to request a copy of our Privacy Notice, which provides more detail on how we may use or disclose information collected in HMIS.

- This form will expire seven years from the date you signed it. You may revoke your consent at any time prior, but your revocation must be provided either in writing or by completing the Revocation of Consent form. The agency you are receiving services from must make this form available to you if you ask. You understand that revoking consent will not change anything about information disclosures that have already occurred.

- If you have any questions or you feel your information has been misused in any way you can contact the Cambridge CoC by emailing PlanningDev@cambridgema.gov or calling 617-349-6206.

SIGNATURE AND ACKNOWLEDGEMENT

By signing below, I affirm that I have read this document, or it was read to/or explained to me and I understand and agree with the terms of this document.
NOTE: If you have a family/household with dependents under age 18, please complete the back of this form as well.

Client Name (printed) _____

Client Signature _____ Date ___/___ /____

Agency Witness/Staff Name _____

Agency Witness/Staff Signature _____ Date ___/___ /____

Agency Name _____

Minor Children (if any):

Name: _____ DOB: ___/___ /____ Name: _____ DOB: ___/___ /____

Name: _____ DOB: ___/___ /____ Name: _____ DOB: ___/___ /____

Name: _____ DOB: ___/___ /____ Name: _____ DOB: ___/___ /____

HMIS Grievance Form

HMIS Clients are encouraged to work with the agency they are having issues with before submitting a grievance. A grievance should be used as a last resort. All grievances are taken very seriously and reviewed by the Cambridge CoC and HMIS Lead on an individual basis.

If you have not been able to resolve your issue with the agency directly, please complete this form.

- Complete all fields
- Print legibly
- Be as specific and as detailed as possible
- Attach additional pages as necessary
- Sign and date the form

If you have any questions about completing this form, please call 617-+349-6966 and speak to the Cambridge HMIS System Administrator.

Grievances must be submitted in writing to:

Planning & Development Office
Department of Human Service Programs
City of Cambridge
51 Inman Street
Cambridge, MA 02139
Attn: HMIS Administrator

Alternatively, this form may be emailed to PlanningDev@Cambridgema.gov

Name of Agency you've been working with to solve the issue:	**Agency Contact Person: list the name of the person you've been working with to solve the issue.**

Cambridge CONTINUUM OF CARE

Description of issue. Please use the space below to describe your issue. Please print legibly and be as detailed as possible. Attach additional pages as needed.

Your Name:	Best way to contact you:
Your Phone #:	Your email address:
Your mailing address:	
CoC Response date:	

Recommendation to Agency:

Cambridge CONTINUUM OF CARE

Cambridge HMIS

Revocation of Consent Form

By signing this form, you revoke your authorization for this agency and the Cambridge Continuum of Care to share basic data about yourself and your household (if applicable).

You understand that your information will remain in HMIS as part of the non-identifying data collected on homeless services provided by the Cambridge Continuum of Care (CoC) and you understand that your information will only be used according to the procedures outlined in the Cambridge HMIS Privacy Notice document. You understand that information that has already been entered will remain in the system. By canceling your agreement for sharing information within the Cambridge HMIS, your personal information that has been saved will be restricted. You further understand that this revocation of data sharing only applies to information within the HMIS. Any information which was shared or retained outside of HMIS is not affected by this revocation. By signing, you acknowledge and understand that this Client Revocation of Consent to Release Information applies only to the sharing of information within the HMIS from this day forward.

You understand that by revoking your refuse consent to share information you will not lose or be denied any benefits or services.

If you have any questions or you feel your information has been misused in any way you can contact the Cambridge HMIS Support staff at 617-349-6966.

Signature:

Client Printed Name	DOB	Date

Client Signature

Agency Witness	Printed Agency Staff Name/Name of Agency

CAMBRIDGE HMIS

User Policy, Responsibility Statement & Code of Ethics

Name (Print)	**Agency Name (Print)**
Work phone	**Email address**

USER POLICY

Agency User recognizes the primary focus in the design and management of the Cambridge HMIS is to address the needs of the clients. This includes both the need to continually improve the quality of homeless and housing services, and the need to maintain client confidentiality by treating personal data with respect and care.

As the guardians entrusted with this personal data, Cambridge HMIS users have a moral and a legal obligation to ensure that appropriate methods are practiced with the collection, access, and utilization of data. Each user is responsible to make sure that client data is only used for the purpose for which it is collected. Proper user training, adherence to the Cambridge HMIS policies and procedures, and a clear understanding of client confidentiality are vital to achieving these goals.

USER RESPONSIBILITY

Your User ID and Password give you access to the HMIS system. Initial each item below to indicate your understanding and acceptance of the proper use of your User ID and password. Failure to uphold the confidentiality standards set forth below is grounds for termination from Cambridge HMIS.

_____ My User ID and Password are for my use only and must not be shared with anyone.

_____ I must take all reasonable means to keep my password physically secure.

_____ I understand that the only individuals who can view information in HMIS are authorized users and the Clients to whom the information pertains.

_____ Under no circumstances will I access confidential information for any purpose other than the performance of my assigned job duties.

_____ If I am logged into HMIS and must leave the work area where the computer is located, I must log-off HMIS before leaving the work area.

_____ Failure to log off HMIS may result in a breach in Client confidentiality and system security.

_____ Hard copies of HMIS information must be kept in a secure file.

_____ When hard copies of HMIS information are no longer needed, they must be properly destroyed to maintain confidentiality.

_____ If I notice or suspect a security breach, I will immediately notify my Agency HMIS Administrator and Cambridge's Planning and Development office (617-349-6966).

_____ I have read and will abide by all policies and procedures in the Cambridge HMIS Policy and Procedures manual.

USER CODE OF ETHICS

A. Users must be prepared to answer client questions regarding Cambridge HMIS.

B. Users must allow client to change his or her information sharing preferences at the client's request.

C. Each User should maintain high standards of professional conduct in the capacity as a HMIS User.

D. The User has primary responsibility for his/her Client(s).

By signing my name and the date, I understand I am agreeing to comply with all the statements listed above.

_____ _____

Signature of HMIS User Date