MA-503 Cape Cod and Island CONTINUUM OF CARE

Homeless Management Information System HMIS POLICIES AND PROCEDURES MANUAL

Version 3.0

UPDATED November 2020

CONTENTS

SECTION 1: HMIS OVERVIEW

Definition of Homeless Management Information System (HMIS)

A Homeless Management Information System (HMIS) is a locally administered electronic data collection tool used to record and store client-level information about the numbers, characteristics, and needs of participants who use homeless housing and supportive services or homelessness prevention services.

HMIS is essential to efforts to coordinate client services and inform community planning and public policy. Through HMIS, homeless individuals benefit from improved coordination within and among agencies, informed advocacy efforts, and policies that result in targeted services. Analysis of information gathered through HMIS is critical to the preparation of a periodic accounting of homelessness in Cape Cod and Islands CoC, including required HUD reporting.

HUD HMIS Requirement

Since 2004, HUD has required recipients of Continuum of Care (CoC) Program funds to collect electronic data on their homeless clients in HMIS. HUD published the HMIS Data and Technical Standards in the Federal Register in 2004, specifying the data elements and standards that guide HMIS data collection across the country, standardizing data collection nationally, and describing how data is to be collected and safeguarded. The HMIS Technical Standards were amended by HUD in 2010. In 2011, HUD published a proposed rule establishing HMIS requirements (76 FR 76917). The proposed rule requires that every CoC have an HMIS that is operated in compliance with the requirements of 24 CFR part 580.

Cape Cod and Islands COC: HMIS Lead and System

The Cape and Islands Regional Network on Homelessness Policy Board has designated Barnstable County as the CoC's HMIS Lead entity. Barnstable County serves as HMIS Administrator/Security Officer to both assure the quality of data entered in the database and to support general usage by all programs using the system. Barnstable County is also responsible for monitoring compliance to HUD Data Standards and policies set within the CoC, for developing necessary reports, and for overseeing privacy and security policies.

The CoC has selected Social Solutions' Efforts to Outcomes (ETO) to serve as the CoC's HMIS software and participates in the MA Department of Housing and Community Development's (DHCD) MAHMIS ETO Enterprise. Each Covered Homeless Organization (CHO) has its own HMIS site and each agency controls its own data sharing. ETO serves as a web-based direct data entry portal for organizations that use ETO as their data

management system. Non-CoC funded CHOs may participate in HMIS using other software products, providing that the software:

- Is capable of collecting HUD Universal and Common Date Elements, and
- Is capable of generating HUD reports in Comma Separated Values (csv) files for upload into the CoC's HMIS.

Covered Homeless Organizations (CHOs)

All Cape and Islands CoC recipients of grants from programs authorized by the HEARTH ACT Program Rule Title IV of the McKinney-Vento Act are required to contribute data to the CoC's HMIS, with the exception of victim service provides.[1] In addition, all other Cape Cod and Islands CoC agencies providing shelter, housing and services to homeless and at-risk populations are strongly encouraged to use the Cape and Islands CoC HMIS database.

An agency that participates in HMIS is referred to as a Covered Homeless Organization (CHO). CHOs are responsible for their client level data, are responsible for the integrity and security of their agency's client level data and assume the liability for any misuse of the system by agency staff. CHOs are responsible for ensuring that their agency users comply with the policies and procedures outlined in this manual.

Governance

The Cape Cod and Islands CoC adopted an HMIS Governance Charter in September 2013 (updated June 2020), which defines the roles and responsibilities of the CoC, the HMIS Lead, CHOs, and the HMIS Committee. These HMIS Policies and Procedures incorporate the terms of the HMIS Governance Charter.

Definitions of Key Terms

The section below defines key terms used throughout this document and HUD guidance regarding HMIS.

- **Client Level Data** – (see **Personal Identifiable Information**, below)

- **Comparable Database -** A database that is not the CoC's official HMIS, but an alternative system that victim service providers and legal services providers may use to collect client-level data over time and to generate unduplicated aggregate reports based on the data, and that complies with the requirements of this part. Information

[1] Victim services providers are prohibited from entering client data into HMIS and must instead enter required data into a comparable database.

entered into a comparable database must not be entered directly into or provided to an HMIS.

- **Continuum of Care (CoC) -** The group composed of representatives from organizations including nonprofit homeless 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 veterans, and homeless and formerly homeless participants organized to carry out the responsibilities of a Continuum of Care established under 24 CFR part 578.

- **Data Recipient -** A person who obtains PII from an HMIS Lead or from a CHO for research or other purposes not directly related to the operation of the HMIS, Continuum of Care, HMIS Lead, or CHO.

- **Homeless Management Information System (HMIS) -** The information system designated by Continuums of Care to comply with the requirements of 24 CFR part 580 and used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness.

- **HMIS Lead** - The entity designated by the Continuum of Care in accordance with 24 CFR part 580 to operate the Continuum's HMIS on its behalf. The HMIS Lead for the Cape Cod and Islands CoC is Barnstable County.

- **HMIS Administrator** – Person responsible for all facets of the day to day operation to maintain the HMIS system and works for the HMIS LEAD.

- **HMIS Vendor** - A contractor who provides materials or services for the operation of an HMIS. An HMIS vendor includes an HMIS software provider, web server host, data warehouse provider, as well as a provider of other information technology or support.

- **Personal Identifiable Information (PII)** - Information about a program participant that can be used to determine a program participant's identity, either when used alone or when combined with other information, such as Name, Date of Birth, Social Security Number, etc. In this manual, the term **Client Level Data** may be used interchangeably with PII.

- **Unduplicated Accounting of Homelessness** - An unduplicated accounting of homelessness includes measuring the extent and nature of homelessness (including an unduplicated count of homeless participants), utilization of homelessness programs over time, and the effectiveness of homelessness programs.

- **User** - An individual who uses or enters data in an HMIS or another administrative database from which data is periodically provided to an HMIS.

- **Victim Service Provider** - A private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. This term includes rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs.

Policy Review and Amendment

On an annual basis, the HMIS Lead and the HMIS Committee will review the HMIS Policy and Procedures Manual to ensure compliance with HUD regulations/technological changes.

If policy changes are necessary, the HMIS Lead will submit recommendations for revisions to CoC Lead staff, who will review the suggested policy updates. The CoC staff will forward recommendations to the Cape Cod and Islands Regional Network Executive Committee, who will in turn present the recommended policy revisions to the Cape Cod and Islands Regional Network Policy Board. The policy revisions will be reviewed and voted on by the Cape Cod and Islands Regional Network Policy Board. The HMIS Lead will modify practices, documentation, and training material to be consistent with the revised policies within six months of approval.

Privacy, Security and Data Quality Plans

The HMIS Lead, in consultation with CHOs and the CoC, is responsible for creation and updating of Privacy, Security, and Data Quality Plans which conform to HUD requirements. These Plans are incorporated into these policies and procedures and must be complied with by the HMIS Lead and all CHOs.

SECTION 2: PARTICIPATION IN HMIS

Contribution of Data

Data are contributed to HMIS in one of two ways:

- Contribute directly to the Cape Cod and Islands CoC HMIS. Agencies that contribute directly are provided web-based log-in information with which to access the system.
- Contribute data to a client management information system operated by a CHO that allows the CHO to collect the minimum required data elements and to meet other established minimum participation thresholds established by HUD. The CHO will work with the HMIS Administrator to securely upload the data from the CHO's system to the Cape and Islands CoC HMIS.

Participation Agreement

All CHOs that participate in the Cape Cod and Islands CoC's ETO/HMIS platform must sign and agree to abide by the terms of the Commonwealth of Massachusetts Department of Housing and Community Development (DHCD) All Services Integrated System Tracker (ASIST) Participation Agreement (Appendix 1). Data from CHOs that do not participate in the CoC's ETO platform will be uploaded to the Massachusetts Rehousing Data Collective (RDC) data warehouse, through which the CoC will have access to the data. These CHOs must sign and agree to abide by the terms of the DHCD RDC Data Sharing Agreement (Appendix 2).

CHO HMIS Site Administrator

Each CHO must designate a single agency representative to act as the CHO's HMIS Site Administrator (Appendix 3). CHO HMIS Site Administrators are responsible for the following:

- Communicate personnel/security changes for HMIS users to the Cape Cod and Islands CoC HMIS Administrator
- Act as the first tier of support for agency HMIS users
- Act as the liaison or contact between the agency and Cape Cod and Islands CoC HMIS Administrator
- Ensure that the agency adheres to client privacy, confidentiality, and security policies
- Maintain compliance with technical requirements for participation
- Store and enforce end user agreements

- Deactivate users who are no longer authorized to have access to HMIS
- Ensure that the Privacy Notice is being used
- Enforce data collection, entry, and quality standards
- Attend trainings and technical assistance as offered.

Technological Requirements for Participation

All computers accessing the Cape Cod and Islands CoC HMIS on behalf of the agency must meet the minimum system requirements as outlined in the HMIS Security Plan, which is incorporated into these policies and procedures.

Agency Profiles in HMIS

Each agency must be set up in HMIS, with profiles that define the programs and services the agency offers, prior to HMIS use and data entry. Agencies should contact the Cape Cod and Islands CoC HMIS Administrator for agency set up. Agency Profiles will be reviewed and updated on an annual basis.

Authorization of HMIS Users - Access to HMIS

To add a new agency MAHMIS ETO User, a CHO must submit a completed copy of the HMIS User Account Request (Appendix 4) to DHCD. By submitting the User Request, the CHO Site Administrator verifies that the new user has completed the necessary privacy and security training. DHCD provides each new ETO HMIS user with a unique username and temporary password. The HMIS user must change the password the first time he/she logs into the system.

Each CHO HMIS Site Administrator should keep an updated list of approved agency users; this document should be submitted to the HMIS Administrator on a quarterly basis. The Authorized User List form is attached to this manual as Appendix 5.

Training

The HMIS Administrator provides initial training to new HMIS users regarding privacy and security measures. All users are required to complete the training module before being issued a password.

The HMIS Administrator offers regular training in system use for CHO HMIS Site Administrators and expects these sessions to operate in a “train-the-trainer” model, in which CHO HMIS Site Administrators will be responsible for training their agency’s HMIS users to use the system for data input.

User Agreements Document Retention

HMIS User Agreements must be signed and kept by CHOs for all agency personnel or volunteers that will collect or use HMIS data on behalf of the agency. Agencies must store original HMIS User Agreements for five (5) years after revoking an individual's authorization or in terminating an individual's employment.

Removing Authorized Personnel

Site Administrators must immediately deactivate user accounts for individuals who are no longer authorized to access HMIS on the agency's behalf. The HMIS Administrator must be notified in writing within one business day of such user terminations and must update the list of authorized users in the HMIS system.

SECTION 3: DATA COLLECTION

Collection of Data on Participants and Non-Participants

Agencies should collect data from families and individuals who are homeless or at risk of becoming homeless and are accessing services from their agency. Agencies may also choose to collect data for HMIS on individuals or families that make contact with the agency but are not able to receive services from the agency. Information must be collected separately for each family member, and all family member data must be entered into the database.

Required Data Elements

The HUD June 2020 HMIS Data Standards outline three categories of required data elements: Project Descriptor Data Elements, Universal Data Elements (Universal Identifier Elements and Universal Project Stay Elements), and Program Specific Data Elements.

Project Descriptor Data Elements

Project descriptor data elements (PDDE) are intended to identify the organization, specific project, and project details to which an individual client record in an HMIS is associated. They are created at initial project setup within the HMIS and should be reviewed at least once annually and as often as needed to ensure that reporting is accurate. The HMIS Lead Agency must ensure that the HMIS includes project descriptor information for all projects participating in HMIS. Project descriptor data elements required for project setup in HMIS include: Organization Identifiers, Project Identifiers, Continuum of Care Code, Project Type, Method for Tracking Emergency Shelter Utilization, Federal Partner Funding Sources, and Bed and Unit Inventory Information.

Universal Data Elements

Universal Data Elements are to be collected by all projects participating in HMIS, regardless of funding source, as part of the Continuum of Care's HMIS implementation. Universal Identifier Elements (one and only one per client record) are: Name, Social Security Number, Date of Birth, Race, Ethnicity, Gender, and Veteran Status. Universal Project Stay Elements (one or more value(s) per client or household project stay) are: Disabling Condition, Project Start Date, Project Exit Date, Destination, Relationship to Head of Household, Client Location, Housing Move-in Date, and Living Situation. ETO automatically generates the unique personal identification number, the program identification number, and household identification number data elements.

Program Specific Data Elements

To meet the statutory and regulatory requirements of federally funded programs using HMIS, additional elements are required for different funding sources. Program Specific

Data Elements are required by some HMIS federal partner programs and are necessary to complete Annual Performance Reports (APRs) required by programs that receive funding under the McKinney-Vento Homeless Assistance Act. Program specific data elements include: Income and Sources, Non-Cash Benefits, Health Insurance, Disability Elements (Physical Disability, Developmental Disability, Chronic Health condition, HIV/AIDS, Mental Health Problem, Substance Abuse), Domestic Violence, Contact, Date of Engagement, Bed-Night Date, and Housing Assessment Disposition. Program specific data elements that are optional for some programs include: Employment, Education, General Health Status, Pregnancy Status, Veteran's Information, Children's Education, Reason for Leaving, and Services Provided. Some of these optional elements may be required for certain programs and funding streams.

HMIS Data Collection Standards and Assessments

Intake and Assessment Forms

Each client record in HMIS requires certain basic information to be entered, including name, date of birth, social security number, gender, race, ethnicity, primary language, and veteran status (all adults). A Client Data Collection Template may be found in Appendix 6.

In addition, there are four HMIS assessments used by the CoC for data collection: Project Entry Assessment (Appendix 7), Annual Assessment, Update Assessment (both Appendix 8), and Exit Assessment (Appendix 9).

All programs must use the Project Entry and Project Exit Assessments. Agencies receiving funds from federal homeless assistance grants are additionally required to use the Project Annual Assessment and Project Update Assessment forms. The CoC urges all CHOs, regardless of funding source, to gather and submit data through all four Assessments to provide a more complete picture of homelessness in the Cape and Islands Region. The additional data points can prove extremely helpful for the agency when reporting on client outcome measurement/progress, internal accounting for service delivered, and external reporting to funders.

It is important to note that project start date and project exit date entered into HMIS must reflect actual dates that the participant entered and exited the program, not the date of data entry or update. In addition, project start date and entry assessment date must match for each participant entered in the program.

Project Entry Assessment

Project Entry Assessment is used for collecting and entering new client data into HMIS and is required for all persons entered in the system.

All CHOs must ensure that clients served are entered into the HMIS with the required data elements and assigned to a program with an entry date and subsequent exit date from the program. The entry and exit dates are required to determine a client's length of stay in the program, the client's patterns of homelessness, and daily capacity rates of the program. Entry and exit dates differ for program types, however the Cape and Islands CoC expects the following standards for each program type.

- **Emergency Shelters for Individuals** are required to enter clients into the program on the first night of stay in the shelter and assigned a bed using the HMIS bed register on a daily basis when residing in the shelter. Individual emergency shelter clients who have been entered into the program on their first night of stay and have not returned after 30 days must be exited from the program using the last night in the bed as the program end date and exit assessment date.
- **Emergency Shelters for Families** are required to enter clients into the program on the first night of stay in the shelter and assigned a bed using the HMIS Emergency Assistance (EA) bed register. Family members departing shelter must be exited out of the program when they leave the program.
- **Transitional Housing Programs** are required to assign entry dates to clients when they move into the program and exit dates when they leave the program.
- **Permanent Supportive Housing Programs** are required to assign Project Start dates and Move In dates for clients and to exit clients when they leave the program, using the required Program Specific Data Elements for both entry and exit.
- **Supportive Service Only Programs** should enter clients with an entry date of first contact with said client and exit the client from their program when the client's case has been closed. Supportive Service only programs are requested to be mindful of which clients are entered into the program through the HMIS. These clients should be actually served by the program and can report outcomes for the client as opposed to capturing data on every client inquiring about the program who may not meet eligibility requirements.

Failure to assign entry and exit dates to a client will result in non-compliance of the Cape Cod HMIS Data Quality Standards and possible loss of points in CoC Competition.

Domestic Violence programs are exempt from this requirement per VAWA section 3 "Universal Grant Conditions: Nondisclosure of Confidential or Private Information" and section 605 "Amendment to the McKinney-Vento Homeless Assistance Act".

Update Assessment

Update Assessments are used when there are changes in a participant's income, benefits, or disability between the Entry Assessment and Exit Assessment. There is no limit to the

number of update assessments that can be entered. Update Assessments use the same data collection template as the Annual Assessments.

Annual Assessment

Although only Continuum of Care-funded programs are required to complete Annual Assessments for all participants each year (within 30 days before or after the participant's project start date anniversary) until the individual or family members exit the program, the CoC urges all CHOs to conduct annual assessments. Ongoing assessments and updating of participant information enables the program and the CoC to assess progress toward housing stability, increased income, and increased access to mainstream benefits.

Project Exit Assessment

The Exit Assessment provides information on the participant's status at exit, as well as the participant's housing destination. Continuum of Care programs must complete exit assessments for all exiting participants. When exiting (dismissing family members or individuals from the program), the exit assessment date must match the dismissal date.

Client Dismissal

All providers, including emergency shelter providers, must dismiss participants as of the actual date of exiting the program. Intermittent participants must be entered and exited from programs for each intermittent stay.

Timeliness of Data Entry

Agencies may choose to enter data directly into the HMIS or to collect client level data on paper prior to entering into HMIS. If agencies use paper data collection forms, all hard copy forms and services must be entered into the database within 48 hours or within 24 hours for emergency shelter providers. Whether direct data entry or paper forms are used, the data collected and entered must be consistent with the data provided by the client and the hard copy data collection form the CoC provides. All hard copy data must be secured following CoC HMIS security and confidentiality policies.

SECTION 4: DATA QUALITY PLAN

Data Quality

The value of HMIS depends on the quality of the data entered into the program. All programs must strive to provide the most accurate and consistent data as is possible.

Reducing Duplicates

Users should ensure that duplicate records are not created within ETO by conducting a thorough client search at intake. If duplicates are created, the CHO must work with the HMIS Lead to merge the duplicate records.

Improving Data Quality

All CHOs must comply with standards set forth in the CoC's Data Quality Plan, which is incorporated into these HMIS Policies and Procedures.

Data Quality Benchmarks and Controls

As part of its data quality plan, the CoC follows the Data Quality Benchmarks found in Appendix 10. The chart identifies the standards that the CoC will monitor, as well as the monitoring procedures for each standard. The Coverage standard applies to the CoC as a whole, while all other standards apply to CHOs and programs.

Roles and Responsibilities

Cape Cod and Islands CoC

The Cape Cod and Islands CoC is responsible for oversight of data quality and will review high-level data quality reports quarterly. The Policy Board will act upon recommendations made by the HMIS Data Committee and the HMIS Lead.

HMIS Committee

The HMIS Committee is responsible for ongoing oversight of progress toward meeting all CoC goals as stated in the Data Quality Plan. The Committee will review data quality reports as requested by the HMIS Lead, review the HMIS Policies and Procedures manual on an annual basis, review Data Quality Benchmarks on an annual basis, review Security and Privacy policies on an annual basis, and convene as necessary to address data quality issues system-wide.

HMIS Lead – Barnstable County

The HMIS Lead is responsible for monitoring CHOs to ensure that the standards for the extent and quality of data entered into HMIS, as set forth in these policies and procedures, are met to the greatest possible extent and that data quality issues are quickly identified and resolved. The HMIS Lead is also responsible for training CHOs and for

providing technical assistance as necessary to complete required reports on a timely basis. Regularity of reporting provides participating agencies with the opportunity to review data and update any missing elements before the HMIS Administrator assesses progress.

The HMIS lead will run system-wide ***Data Validation Errors Report*** the first week of every month and provide to the Regional Network on Homelessness Policy Board Executive Committee (EC) a Data Quality report at each monthly meeting. This report will be made available for CoC program performance monitoring. CHOs will be notified of data quality problems by the HMIS Lead with recommendations for resolution:

- ***Missing / Incomplete Project Descriptors:*** CHO has failed to set up Project Descriptor Data Elements in HMIS, or Project Descriptor Data Elements are incomplete.
- ***Missing / Incomplete Data Elements:*** CHO has failed to enter complete universal and/or program specific data elements.
- ***Missing / Incomplete Assessments***: CHO has failed to record required assessments (entry, update, annual exit), or detailed information is missing from project assessments.
- ***Warnings:*** CHO has recorded incomplete responses which are considered as "No Response" by HUD reporting standards.

The HMIS Administrator will train one person from each CHO to run the Data Validation Errors Report for all the agency's projects. This report should be run the first week of every month by the CHO and used to identify areas of inaccurate, incomplete, or missing data.

Progress reports on expected contractual outcomes will be developed to track each funded project's specific target requirements. Such reports are intended to show the agency's progress to date on their contractual agreements. Both the dates and methods of tracking information will vary according to the particular project.

As part of the ***CoC Annual Grantee Site Visit***, the HMIS Administrator will monitor the CoC-funded projects to review data quality reports, bed utilization reports, and compliance with the Data Quality Plan; will report to the HMIS Committee on the quality and usability of data submitted by CoC-funded agencies; and will make recommendations to the HMIS Committee for improvements in data quality.

Covered Homeless Organizations

CHOs are responsible for training and monitoring HMIS users to ensure understanding of and compliance with data quality standards.

Each CHO is responsible for addressing any issues identified through the data quality

monitoring. Where data errors are identified, the CHO must correct the errors within five (5) days or contact the HMIS lead if they need more time or additional assistance. Where overall systemic data quality issues are identified, the CHO must participate with the HMIS Lead in creation of a corrective action plan.

Remedial Actions

The CoC's goal of data quality monitoring is to obtain and maintain high-quality data. In order to meet this goal, CHOs with repeated data quality issues will be initially provided with increasing levels of support to assist in resolving data issues. Support may include additional training and/or technical assistance from the HMIS Lead.

The CHO may be required to submit a corrective action plan to the HMIS Lead and to provide regular reports to the HMIS Lead on progress toward implementing the identified corrective actions. Components of a corrective action plan may include:

- Developing and following a schedule of actions for carrying out HMIS-related tasks, including schedules, timetables, and milestones
- Establishing and following an HMIS data quality plan that assigns responsibilities for carrying out remedial actions
- Increased monitoring and reporting of HMIS data quality.

If increased support does not result in the CHO meeting data quality standards, the CHO may be subject to sanctions, as described in Section 4 of this HMIS Policies and Procedures Manual.

SECTION 5: COMPLIANCE, TECHNICAL ASSISTANCE, AND SANCTIONS

The goal of the CoC and the HMIS Lead is to ensure that all CHOs are in compliance with all requirements and are using HMIS to improve services to participants.

Compliance and Technical Assistance

CHOs are required to comply with these policies and procedures and with HMIS Privacy, Security, and Data Quality Plans. If CHOs have difficulty achieving compliance, the HMIS Lead will provide technical assistance. The CHO may request technical assistance, or the HMIS may offer it.

CHOs are subject to annual HMIS monitoring. If compliance issues are identified through monitoring or become apparent between monitoring, the HMIS will request that the CHO provide a plan for coming into compliance, and the HMIS Lead will monitor progress toward meeting requirements of the plan.

Sanctions

In the event of violations of privacy or confidentiality standards, or ongoing failure to meet data quality standards, sanctions may be warranted. Violations must be reported to the HUD Regional Office.

Potential sanctions may be imposed by HUD and include the following:

- Suspending funds disbursement
- Suspending or terminating access to HMIS
- Reducing or terminating the remaining grant
- Imposing conditions on future grants
- Imposing other legally available remedies.

CHOs subject to sanctions may not apply for new CoC Program or Emergency Solutions Grant Program funds. CHOs who have lost access to the Cape Cod and Islands CoC HMIS due to sanctions may not apply for CoC Program renewal funds.

An initial recommendation that sanctions be imposed is generated by the HMIS Lead and is presented to the Executive Committee. The Executive Committee will make a recommendation to the Policy Board and the Collaborative Applicant will notify the HUD Regional Office.

Compliance and Project Review for Renewal

Compliance with the policies and procedures set forth in this manual and the level of data quality achieved will be reported to the CoC Review and Ranking Committee, which may take these factors into consideration in determining which projects will be submitted for renewal and which agencies

may be permitted to apply for new project funding. Decisions of the CoC Ranking and Review Committee are separate and distinct from decisions concerning imposition of sanctions.

SECTION 6: SECURITY PLAN

Security Officers

The Cape Cod and Islands CoC has designated the HMIS lead as the HMIS Security Officer. The duties include:

- Review of the Security Plan annually or anytime there is a change to the security management process, software, methods of data exchange, and any HMIS data or technical requirements issued by HUD. If changes are required to the HMIS Security Plan, the Security Officer will work with the HMIS Committee for review, modification, and approval.
- Confirmation that the Cape Cod and Islands CoC HMIS adheres to the Security Plan.
- Response to any security questions, requests, or security breaches to the Cape and Islands CoC HMIS and communication of security related HMIS information to CHOs.

Identification of CHO HMIS Security Officer

Each CHO must also designate a CHO HMIS Security Officer (Appendix 11) whose duties include:

- Confirmation that the CHO adheres to the Security Plan.
- Communication of any security questions, requests, or security breaches to the Cape Cod and islands CoC HMIS Security Officer, and security related HMIS information relayed from the Cape Cod and the Islands HMIS System Administrator to the CHO's end users.
- Participate in security training offered by the Cape Cod and Islands CoC is mandatory and conducted annually.

Annual Security Certification

The Cape Cod and Islands CoC and each CHO must complete an annual security review to ensure the implementation of the security requirements for the HMIS. This security review must include completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan. If the requirement cannot be met at the time of the initial certification, the Security Officer must indicate a date not later than three months after the initial certification by which the requirement will have been met. At that time, the Security Officer will be required to submit an updated version of this form demonstrating compliance. All CHO Security Officers must complete the Security Compliance Certification (Appendix 12) every January and submit the completed form to the CoC Security Officer no later than February 15 of each year.

Security Awareness Training and Follow-up

All users of the HMIS must receive security and privacy training prior to the submission of their ETO New User Request to DHCD by the CHO's Site Administrator. The request for New User access requires certification that the user has completed the on-line security training. CHOs that do not participate in the MAHMIS ETO platform should confirm in writing to the HMIS Administrator that staff who have access to data that will be uploaded to the CoC's HMIS have completed the online security training. In addition, the Cape Cod and Islands CoC shall provide security training no less than once per year.

Reporting Security Incidents

The HMIS Lead has created the following policy and chain of communication for reporting and responding to security incidents.

Security Incidents

All HMIS users are obligated to report to their agency HMIS Security Officer suspected instances of noncompliance with policies and procedures that may leave HMIS data vulnerable to intrusion. Each CHO is responsible for reporting any security incidents involving the real or potential intrusion of the Cape Cod and Islands HMIS ETO software. The Cape Cod and Islands CoC is responsible for reporting any security incidents involving the real or potential intrusion of the Cape Cod and Islands CoC ETO HMIS system to the Regional Network on Homelessness Executive Committee.

Reporting Threshold

HMIS users must report any incident in which unauthorized use or disclosure of PII has occurred and any incident in which PII may have been used in a manner inconsistent with the CHO Privacy or Security Policies. Security breaches that have the possibility to impact the Cape Cod and Islands CoC HMIS and must be reported to the HMIS Lead.

Reporting Process

HMIS users will report security violations to their CHO HMIS Security Officer. The CHO HMIS Security Officer will report violations to the Cape Cod and Islands HMIS Administrator. Any security breaches identified by Social Solutions ETO will be communicated to the Cape Cod and Islands CoC HMIS Administrator. The HMIS Administrator will review violations and recommend corrective and disciplinary actions to the CHO as appropriate. Each CHO will maintain and follow procedures related to internal reporting of security incidents.

Audit Controls

Social Solutions maintains an accessible audit trail within ETO that allows the HMIS Administrator to monitor user activity and examine data access for specified users. The HMIS Administrator will monitor audit reports for any apparent security breaches or behavior inconsistent with the Privacy Policy outlined in these policies and procedures.

System Security

Each CHO must apply system security provisions to all the systems where PII is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini- computers, mainframes and servers.

User Authentication

A CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

Virus Protection

A CHO must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

Firewalls

A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall if there is a firewall between that workstation and any outside systems, including the Internet and other computer networks. For example, a workstation that accesses the Internet through a modem needs its own firewall. A workstation that accesses the Internet through a central server does not need a firewall if the server has a firewall.

Physical Access to Systems with Access to HMIS Data

A CHO must ensure that computers stationed in public areas that are used to collect and store HMIS data are staffed at all times. When workstations are not in use and staff is not present, steps should be taken to ensure that computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.

Hard Copy Security

A CHO must secure any paper or other hard copy containing PII that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PII when

the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.

Hard copies of data stored or intended to be stored in HMIS, regardless of whether the data has yet been entered into HMIS, will be treated in the following manner:

1. Records shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, records shall be maintained in such a manner as to prevent exposure of PII to anyone other than the user directly utilizing the record.
3. Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the CHO's place of business and where return of the records by the close of business of would result in the undue burden on staff.
4. When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not re-disclose the PII contained in those records except as permitted by these policies and procedures.
5. Faxes or other printed documents containing PII shall not be left unattended.
6. Fax machines and printers shall be kept in secure areas.
7. When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
8. When finished faxing, copying or printing all documents containing PII should be removed from the machines promptly.

Electronic Communication

All electronic communications containing PII retrieved from the HMIS or collected and stored in hard copy format for entry into HMIS must be sent via encrypted email. No client-level HMIS data may be sent electronically unless the transmission is secured through encryption.

Database Integrity

The CHO must not intentionally cause corruption of the Cape Cod and Island HMIS in any manner. Any unauthorized access or unauthorized modification to computer system information or interference with normal system operations will result in immediate suspension of HMIS licenses held by the CHO and suspension of continued access to the Cape Cod and Islands HMIS by the CHO.

The Cape Cod and Islands CoC will investigate all potential violations of any security protocols. Any user found to be in violation of security protocols will be subject to sanctions, as described in the HMIS Policies and Procedures Manual. Individual users may be subject to disciplinary action by the employer CHO.

Disaster Recovery

Cape Cod and Islands CoC HMIS data must be stored by the HMIS software vendor in secure and protected off-site locations with duplicate back-up. In the event of disaster, the HMIS Administrator will coordinate with the vendor to ensure the HMIS is functional and that data is restored. The Cape Cod and Islands CoC will communicate to CHOs when data becomes accessible following a disaster.

Contracts and other arrangements

DHCD, as Administrator of the MAHMIS ETO Enterprise and of the Massachusetts Rehousing Data Collective, shall retain copies of all contracts and agreements executed as part of the administration and management of the HMIS and/or necessary to comply with HUD requirements.

SECTION 7: PRIVACY PLAN AND NOTICE SIGN

Data Collection Notice

Agencies that contribute HMIS data must let clients know that PII is being collected, and the reasons for taking this information. A sample data collection notice may be found in Appendix 13. The sample sets forth the explanatory language in English and Spanish and may be posted to meet the notice requirement. While the posted notice is the minimum requirement, agencies may choose to take additional steps to obtain consent from clients, including obtaining written consent. Agencies that provide transitional or permanent housing are encouraged to obtain written consent.

Privacy Notice

Each agency is required to publish and post on its web site a Privacy Notice describing its policies and practices for use of protected personal information and must provide a copy of its Privacy Notice to any individual upon request. The agency must post a sign stating the availability of its Privacy Notice to any individual who requests a copy. Sample Privacy Notices may be found in Appendix 14 (English) and Appendix 15 (Spanish). These documents may be used as is or adapted to each specific agency.

Accountability

Agencies must require staff to sign an agreement that acknowledges receipt of a copy of the Privacy Notice and that pledges to comply with the Privacy Notice. A CHO must establish a written policy for accepting and considering questions or complaints about its privacy and security policies and practices.

Access and Correction

In general, agencies must allow an individual to inspect and to have a copy of any information about the individual and must offer to explain any information that the individual may not understand. Agencies must consider any request by an individual for correction of inaccurate or incomplete information about the individual but is not required to remove any information. However, the agency may mark information as inaccurate or incomplete and may supplement it with additional information.

The agency may deny access to personal reasons for any of the following reasons, and should describe possible reasons in its Privacy Notice:

1. Information compiled in reasonable anticipation of litigation
2. Information about another individual
3. Information obtained under a promise of confidentiality if disclosure would reveal

the source of the information

4. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

The agency can reject repeated or harassing requests for access or correction. An agency that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Purpose and Use Limitations

Agencies may use or disclose PII from HMIS under the following circumstances: (1) To provide or coordinate services to an individual; (2) for functions related to payment or reimbursement for services; (3) to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or (4) for creating de-identified PII.

Certain disclosures may be required due to provider obligations that go beyond the privacy interests of clients. The following additional uses and disclosures are recognized by HUD, and the HMIS Lead may provide additional guidance regarding these circumstances (each of which is described in more detail in the HUD 2004 HMIS Technical Standards):

1. Uses and disclosures required by law
2. Uses and disclosures to avert a serious threat to health or safety
3. Uses and disclosures about victims of abuse, neglect or domestic violence
4. Uses and disclosures for academic research purposes
5. Disclosures for law enforcement purposes

Confidentiality

Each agency must develop and implement written procedures to ensure: (1) All records containing protected Identifiable information of any individual or family who applies for and/or receives Continuum of Care assistance will be kept secure and confidential; (2) The address or location of any family violence project assisted with Continuum of Care funds will not be made public, except with written authorization of the person responsible for the operation of the project; and (3) The address or location of any housing of a program participant will not be made public, except as provided under a preexisting privacy policy of the recipient or subrecipient and consistent with State and local laws regarding privacy and obligations of confidentiality.

Protections for victims of domestic violence, dating violence, sexual assault, and stalking

Victim service providers are prohibited from entering data into HMIS. Other agencies must be particularly aware of the need for confidentiality regarding information about persons who are victims of domestic violence, dating violence, sexual assault, and stalking. Additional protections for these clients include explicit training for staff handling PII of the potentially dangerous circumstances that may be created by improper release of this information.

Other Requirements

All agencies that contribute HMIS data must comply with the baseline privacy requirements described in this Privacy Plan. A CHO must comply with federal, state and local laws that require additional confidentiality protections. When a privacy or security standard conflicts with other Federal, state, and local laws to which the CHO must adhere, the CHO must contact the Cape Cod and Islands HMIS Administrator and collaboratively update the applicable policies for the CHO to accurately reflect the additional protections.

APPENDIX 1: DHCD ASIST HMIS PARTICIPATION AGREEMENT

Massachusetts "All Services Integrated System Tracker" (ASIST)
Homeless Management Information System (HMIS)

Participation Agreement between the Massachusetts Department of Housing & Community Development (DHCD) and

_____
(Agency/Site Name)

This Agreement is entered into between the Massachusetts Department of Housing & Community Development, hereafter referred to as "DHCD" and the above-named service provider, hereafter referred to as "Site," regarding access and use of the Massachusetts Homeless Management Information System, hereafter referred to as "ASIST HMIS."

I. Introduction

The ASIST HMIS, a shared database hosted by Social Solutions, Inc., allows authorized personnel in participating homeless and human service provider agencies throughout the Commonwealth of Massachusetts to enter, track, and report on information concerning their applicants for and recipients of benefits or services administered by or funded through such agencies. In addition, the ASIST EA database will also be hosted by Social Solutions, Inc. and will be used by DHCD staff to determine eligibility for Emergency Assistance programs and benefits. The goals of the ASIST HMIS are to:

- Improve coordinated care for and services to homeless persons in the Commonwealth of Massachusetts,
- Provide a user-friendly automated records system that expedites intake procedures for applicants for and recipients of benefits and services, improves referral accuracy and supports the collection and maintenance of information that can be used for program improvement and service-planning and
- Meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD), the Regional Networks established through the Interagency Council on Housing and Homelessness (hereinafter "Regional Networks"), DHCD and other funding sources as needed.

In compliance with all state and federal requirements regarding privacy, confidentiality, and data security of at-risk-of-becoming homeless, homeless, and formerly homeless or at-risk-of-becoming homeless applicants for and recipients of benefits or services provided by DHCD and by cooperating state, federal, and local agencies, and nonprofit organization, ASIST HMIS is designed to collect and deliver timely, credible, quality data about services and homeless persons or persons at risk for being homeless.

II. DHCD Responsibilities

A. DHCD assumes financial and administrative responsibility for its DHCD-funded programs.

B. DHCD will provide one-time transition support for migrating SHORE data into the Social Solutions, Inc. ASIST HMIS enterprise data base.

C. DHCD will provide model Privacy Notices and other templates for agreements that may be adopted or adapted by the Site to implement ASIST HMIS functions.

D. DHCD or a DHCD-authorized vendor will provide both initial training and periodic training updates for core Site Staff regarding the use of ASIST HMIS, with the understanding that the Site or its designee will take responsibility for conveying this information to all Site Staff using the system. All DHCD sponsored trainings will be a "Train the Trainer" model so that core Site Staff will assume responsibility for further training of additional Site staff.

E. To the extent required by its agreements with Social Solutions, Inc., DHCD will assist Social Solutions, Inc. in providing basic user support and technical assistance (i.e., general trouble-shooting and assistance with standard report generation) to the designated Site Administrator. Access to this basic technical assistance will available in accordance with agreements between DHCD and Social Solutions, Inc. It is expected, but not required, that such basic technical assistance will normally be available from 9:00 a.m. to 5:00 p.m. Monday through Friday (with the exclusion of holidays). ASIST HMIS staff, whether provided through DHCD, Social Solutions, Inc., or another DHCD-authorized vendor, will be accessible for basic technical assistance in accord with procedures that will be published and periodically updated by DHCD.

F. DHCD will not publish reports on data concerning or provided by applicants for and recipients of benefits and services that identify specific persons. Public reports, including but not limited to the HUD Annual Homeless Assessment Report (AHAR) as required by Congress, will be limited to presentation of aggregated data within the ASIST HMIS database.

G. The publication practices of DHCD will be governed by policies established by relevant committees for statewide analysis and will include qualifiers such as coverage levels or other issues necessary to clarify the meaning of published findings.

III. Site Responsibilities

A. The Site Executive Director or authorized signatory will be responsible for entering into applicable fiduciary and administrative agreements for all non-DHCD funded programs through their Continuums of Care (CoC's) and/or Regional Networks.

B. The Site Executive Director or authorized signatory will establish all sharing agreements/protocols for all information to be shared across CoC's, sites/agencies/programs.

C. The Site Executive Director or authorized signatory will be responsible for keeping a record of all end-user/staff agreements, privacy and ethics training sign-offs, Criminal Offender Record Information ("CORI") checks and any other applicable records on site.

D. Data Entry and Regular Use of the ASIST HMIS

1. The Site Executive Director or authorized signatory will designate at least one Site Administrator who will assume responsibility for providing ongoing end-user support to all users within the Site including but not limited to the training of any staff person prior to issuance of a user account. Said designee will be identified to DHCD ASIST HMIS Staff upon designation and when the designee changes.
2. The Site will enter all minimum required data elements as defined for all persons who are participating in services funded by DHCD or the U.S. Department of Housing and Urban

Development (HUD) Supportive Housing Program, Shelter + Care Program, or DHCD/HUD Emergency Shelter Grant Program.

3. The Site will enter data in a consistent manner, and will strive for real-time, or close to real-time, data entry.
4. The Site Administrator will routinely review records the site has entered in the ASIST HMIS for completeness and data accuracy. The review and data correction process will be conducted according to ASIST HMIS policies and procedures.
5. The Site will not knowingly enter inaccurate information into the ASIST HMIS.
6. The Site will review and assess data entered into the ASIST HMIS, and will enter data revisions as necessary, to reflect a change in the status of an applicant for or recipient of benefits or services, enter updates, or edit incorrect information.
7. The Site will prohibit anyone with a Site-assigned User ID and Password from entering offensive language, profanity, or discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation.
8. The Site, including its authorized and unauthorized employees/agents, will utilize the ASIST HMIS and data entered therein for business purposes only.
9. The Site will keep updated virus protection software on Site computers that access the ASIST HMIS.
10. Transmission of material in violation of any United States Federal or State regulations is prohibited.
11. The Site, including its authorized and unauthorized employees, agents, and assigns, and the employees, agents, and assigns of its contractors and subcontractors, will not use the ASIST HMIS with intent to defraud the Federal, State, or local government, or an individual entity, or to conduct any other illegal activity.
12. The Site will incorporate procedures for responding to concerns of applicants for and recipients of benefits and services regarding use of the ASIST HMIS into its existing Program Grievance Policies. While appeals relating to the ASIST HMIS should not be considered part of the Site's formal process, a copy of any ASIST HMIS-related grievance, and the Site's response, must be submitted to the DHCD Project Manager quarterly.
13. Notwithstanding any other provision of this Participation Agreement, the Site agrees to abide by all policies and procedures relevant to the use of the ASIST HMIS that DHCD publishes from time to time.

E. Protection of Privacy of Applicants for and Recipients of Benefits and Services

1. The Site will comply with all applicable federal and state laws regarding protection of privacy and confidentiality of applicants for and recipients of benefits or services, including but not limited to Massachusetts General Laws Chapters 66A and 93H and regulations issued pursuant thereto.
2. The Site 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.
3. The Site will comply specifically with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R., Parts 160 & 164, and corresponding regulations established by the U.S. Department of Health and Human Services .

4. The Site will comply with 201 CMR 17:00 STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH and with Massachusetts Executive Order 504.
5. The Site will comply with all policies and procedures established by DHCD pertaining to protection of privacy, confidentiality, and data security of applicants for and recipients of benefits and services.

F. Confidentiality of Applicants for and Recipients of Benefits and Services

1. The Site agrees to provide a copy of the ASIST HMIS Privacy Notice (or a DHCD-approved Site-specific alternative) to each applicant for and recipients of benefits or services. The Site will provide consumers with an oral explanation of the ASIST HMIS and arrange for a qualified interpreter/translator in the event that an individual is not literate in English or has difficulty understanding the Privacy Notice.
2. The Site will not divulge any confidential information received from the ASIST HMIS to any organization or person without proper written consent by the applicant for or recipients of benefits or services, unless otherwise required or permitted by applicable regulations or statutes.
3. The Site will ensure that all persons who are issued an ASIST HMIS User Identification and Password abide by this Participation Agreement, including all associated confidentiality provisions. The Site will be responsible for oversight and enforcement of its own related confidentiality requirements.
4. The Site will ensure that all persons issued a User ID and Password will complete a formal training on privacy and confidentiality and demonstrate mastery of that information, prior to activation of their User License or accessing the ASIST HMIS.
5. The Site agrees that those granted Site Administrator systems access must first become a Certified Site Administrator through training provided directly by Social Solutions, Inc. and/or by DHCD or DHCD-designated trainers.
6. The Site acknowledges that ensuring the confidentiality, security and privacy of any information downloaded from the system by the Site is strictly the responsibility of the Site.

G. Publication of Reports

1. The Site agrees that it may only release aggregated information generated by the ASIST HMIS that is specific to its own services.
2. The Site acknowledges that the release of aggregated information will be governed through policies established by relevant committees for statewide analysis; the Continuum of Care level for community-level analysis; or the Regional level for regional-level analysis. Such information will include qualifiers as to coverage levels or other issues necessary to fully explain the published findings.

H. Database Integrity

1. The Site will not share assigned User IDs and Passwords to access the ASIST HMIS with any other organization, governmental entity, business, or individual.
2. The Site will not intentionally cause corruption of the ASIST HMIS in any manner. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, may result in immediate suspension of services and, where appropriate, legal action against the offending entities and individuals.

3. The Site will adopt systems and protocols to ensure that its employees, agents, and assigns, and the employees, agents, and assigns of its contractors and subcontractors will adhere to and comply with the Site's obligations under this Agreement.

IV. Hold Harmless

1. DHCD makes no warranties, expressed or implied. The Site at all times, will indemnify and hold DHCD harmless from any damages, liabilities, claims, and expenses that may be claimed against the Site, Social Solutions, Inc., or DHCD, to the extent that such liability arises out of or in regard to the Site's operation of, involvement with, or relation to ASIST HMIS; or for injuries or damages to the Site or another party arising from participation in the ASIST HMIS; or arising from any acts, omissions, neglect, or fault, including but not limited to willful or reckless misconduct, of the Site or its agents, employees, licensees, or assigns, its contractors' or subcontractors' agents, employees, licensees, assigns, or applicants for and recipients of benefits or services; or arising from the Site's failure to comply with laws, statutes, ordinances, or regulations applicable to it or to the conduct of its business. The Site will also hold DHCD harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by the Site's or another participating Site's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/or acts of God. DHCD shall not be liable to the Site for damages, losses, or injuries to the Site or another party other than if such is the result of gross negligence or willful misconduct of DHCD. DHCD agrees to hold the Site harmless from any damages, liabilities, claims or expenses caused solely by the gross negligence or willful misconduct of DHCD.
2. The Site agrees to keep in force a comprehensive general liability insurance policy with combined single limit coverage of not less than five hundred thousand dollars ($500,000). Said insurance policy shall include coverage for theft or damage of the Site's ASIST HMIS-related hardware and software, as well as coverage of Site's indemnification obligations under this Agreement.
3. The provisions of this Section shall survive any termination of the Participation Agreement.

V. General Terms and Conditions

1. The parties hereto agree that this Agreement is the complete and exclusive statement of the agreement between the parties and supersedes all prior agreements, proposals and understandings, oral and written, relating to the subject matter of this Agreement.
2. All data inputted into the ASIST HMIS and all reports generated from such data shall be the intellectual property of DHCD and may only be used consistent with this Agreement and DHCD guidelines. The Site shall not transfer or assign any rights or obligations under the Agreement without the written consent of DHCD.
3. This Agreement commences as of the date of the last signature, and shall remain in force until revoked in writing by either party, with 30 days advance written notice, provided, however, that if allegations or actual incidents arise regarding possible or actual breeches of this Agreement, DHCD may immediately suspend the Site's access to the ASIST HMIS until the allegations are resolved in order to protect the integrity of the system.
4. This Agreement may be modified or amended only by written agreement executed by all parties.
5. DHCD may assign this Agreement upon due notice to the Site.
6. The parties agree that DHCD may perform periodic audits pursuant to DHCD policies to verify the Site's compliance with the requirements of the Agreement.
7. Unless otherwise notified in writing, any communications or notifications among the parties in regard to this Agreement shall be made to the individuals signing below for each party

8. This Agreement is governed by the law of the Commonwealth of Massachusetts. The sole venue for the resolution of any dispute arising out of this Agreement shall be Suffolk County, Massachusetts.

IN WITNESS WHEREOF, the parties have entered into this Agreement by subscribing thereto their hands and seals:

SITE:

For: _____
(Name of Site)

By: _____
(Signature of Authorized Individual)

_____
(Print name)

Title: _____

Date: _____

For: The ASIST HMIS, Department of Housing & Community Development

By: _____
(Signature of Authorized Individual)

_____
(Print name)

Title: _____

Date: _____

APPENDIX 2: REHOUSING DATA COLLECTIVE DATA SHARING AGREEMENT

Commonwealth of Massachusetts
DEPARTMENT OF HOUSING & COMMUNITY DEVELOPMENT
Charles D. Baker, Governor ◆ Karyn E. Polito, Lt. Governor ◆ Jennifer D. Maddox, Undersecretary

REHOUSING DATA COLLECTIVE
DATA SHARING AGREEMENT
BETWEEN
DEPARTMENT OF HOUSING AND COMMUNITY DEVELOPMENT (DHCD)
AND

PROVIDER ORGANIZATION

This agreement is entered into by the Department of Housing and Community Development (DHCD), 100 Cambridge Street, Boston, MA 02114 and _____ Provider Organization (The Partner).

WHEREAS, The Partner is providing services and benefits to homeless households (Clients) with the objective of stabilizing client housing needs and supporting client well-being. The Partner collects and maintains information related to these households, however, Provider organization has no ability to integrate data with the local Continuum of Care (CoC).

WHEREAS, to better inform CoC policy decisions and facilitate HUD reporting, it was determined that all the information related to homeless households should be integrated into one centralized data warehouse, allowing Partner to share data with the local CoC to improve compliance with reporting requirements, and coordinate services and benefits; and

WHEREAS, to this end, a state-wide data warehouse, known as the Rehousing Data Collective (RDC), has been developed and is being administered by the Department of Housing and Community Development; and

WHEREAS, the RDC collects data from participating Provider Organizations, and other entities serving homeless households; and

WHEREAS, data entered into the RDC will be integrated and de-duplicated and result in two data sets- anonymous and de-identified data for public use, and personal and identifiable data for CoC and Provider Organizations use: and

WHEREAS, all data collected about Clients will be entered into the RDC and will be used for reporting, but individual Client data can only be searched or viewed by Provider End Users if the Client has granted permission with a signed Release of Information (ROI).

100 Cambridge Street, Suite 300
Boston, Massachusetts 02114

www.mass.gov/dhcd
617.573.1100

NOW THERFORE, the parties agree as follows:

1. Words capitalized in this agreement shall have the meaning ascribed to them in the definitions contained in **Attachment 1**.

2. DHCD's responsibilities include:

A. Custodian of the Rehousing Data Collective. DHCD will administer the contract with the software reseller (SHI) and work with the software vendor (Green River), to make any necessary changes to the RDC, notify all participating entities about upcoming changes, and maintain the data in accordance with G.L. c. 66A, G.L. c. 93 H, and the Commonwealth's Enterprise Information Security Policy (https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards).

B. Administration of access to warehouse data, including approval of accounts. DHCD, as the RDC Administrator, will approve all Authorized User accounts. CoCs will submit requests directly to the RDC Administrator who will determine if the request can be approved for the type of use requested. The RDC Administrator will verify that the person is an allowable type of user and has completed the required training. All Authorized Users must sign an "RDC User Agreement" that outlines basic privacy and security policies applicable to the user, and must complete the on-line training before the user can access Personal Identifying Information (PII).

C. Monitoring of ROIs. ROIs provide clients with a choice of having their PII shared: 1) state-wide with all other CoCs, 2) only within certain regions, or 3) with no other entities. The RDC Administrator will ensure that data is viewed only by entities specified in the ROI.

D. Funding and resource management. Funds allocated to the RDC project will be administered by DHCD.

E. Training. The RDC has been configured so that no person will be given access to the RDC until that person has completed on-line training related to data security and use of the system. Training for Authorized Users must be renewed every year.

F. System Use Audits. The ReHousing Data Collective records data access information for systems auditing purposes. The Administrator will generate and review audit reports on a regular basis to monitor: 1) users are accessing and/or attempting to access data for authorized purposes, 2) data quality issues impacting the warehouse's ability to report accurate data and trends, and 3) ROI information is complete.

G. Client Complaint Resolution. Client complaints will be addressed as outlined in the policies and procedures manual.

H. Merging of Duplicated Records - Client records that are flagged for merging by End Users will be reviewed by the Administrator for approval.

I. Facilitating the Governance Committee. DHCD will Chair and convene the ReHousing Data Collective Governance Committee on an as needed basis.

3. The Partner's responsibilities include:

A. Recommend Authorized Users. To protect the data maintained in the RDC, only Authorized Users will be given access to the RDC, and Authorized Users will be given different levels of access, depending on the role they have been assigned. The Partner will recommend and endorse individuals who will fulfill the following roles, which are described in more detail in **Attachment 2**:

- RDC Uploader. Partner may request RDC Uploader Accounts for CoC HMIS Leads as well as staff employed at Provider Organizations within the CoC who do not participate in the Continuum's HMIS, but utilize an HMIS-compliant database. These accounts may only be accessed by staff that fulfill specific roles within the agency, which include: CoC HMIS Lead, HMIS Administrator at a Provider Organization, or Executive Director at a Provider Organization.

- CoC End User. The Partner may request CoC End User accounts for the purpose of HUD and CoC reporting to staff persons that fulfill the following roles for a CoC: CoC Designated HMIS Lead Agency, or CoC Designated Collaborative Applicant. CoCs may also request time-limited temporary CoC End User access for the purposes stated in Section 4 to CoC consultants hired to assist with HUD or CoC reporting.

- Provider End User. The Partner may request Provider End User Accounts only for staff at Provider Organizations within a CoC that have been approved by the Partner's Board. The Partner may also request Provider End User accounts for CoC staff who do not work for an HMIS-Participating Organization, but who fulfill the following Coordinated Entry-related roles within the Continuum: Coordinated Entry Triage, or Coordinated Entry Intake points. Provider End User accounts will only be granted to staff who need to complete the tasks listed in Section 4.

B. Upload Data. Initially, upload full HMIS datasets into the RDC from 10/1/2012 to the present in CSV format. Thereafter, import HMIS datasets to the RDC on the agreed upon schedule.

C. Inform the RDC Administrator when the accounts of Authorized Users should be de-activated because the employee left the organization, poses a security risk or for any other reason.

D. Develop and enforce policies to ensure that: 1) individuals for whom Authorized User credentials will be requested have been screened and been determined to pose no security risk, 2) only Authorized Users access the RDC, and, 3) Authorized Users only use the data for the purposes set out in Section 4.

E. Assist clients in understanding the Release of Information (ROI), assist clients in determining which data sharing option is best for them, obtain client signatures on the ROI, and upload the signed ROI to the RDC.

4. Authorized Users will have access to the PII in the RDC **only** for the following purposes:

- To generate CoC Reports for the CoC.
- To perform client level searches to identify individuals in order to obtain a signed ROI.
- To perform client level searches to identify program history for individuals who have signed a ROI.
- Research projects, as agreed upon by the CoCs and DHCD on a case by case basis

5. Authorized Users will be permitted to access data as follows:

A. RDC Administrator will have access to all data contained within the RDC.

B. RDC Uploaders will have access to all data that originated from their own organization's uploads.

C. CoC End Users who generate a Data Report from the RDC will be able to view the data of their CoC's clients' PII in a "drill down" to assist with data quality checks.

D. Provider and CoC End Users will have the ability to view limited Client PII and program enrollment information to obtain a signed ROI for purposes of Coordinated Entry, assistance with service delivery, or generation of the Client-Level System Use and Length of Time Homeless Report mandated by HUD.

6. Access to the RDC will provide Authorized Users with information concerning program participants' personal data as defined by G.L. c. 66A, § 1 or personal information as defined by G.L. c. 93H, § 1. A complete description of the information available in the RDC, including specific data fields or other appropriate descriptors is attached hereto as **Attachment 3**.

7. The Partner and DHCD will take all necessary steps to ensure the confidentiality and security of all PII is maintained in accordance with G.L. c. 66A, G.L. c. 93 H, and the Commonwealth's Enterprise Information Security Policy (**https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards**). The Partner and DHCD will ensure that any PII transmitted electronically or through a portable device be properly encrypted using (at a minimum) the National Institute of Standards and Technology's AES-256 standard and will comply with G.L. c. 93I for the proper disposal of all paper and electronic media, backups or systems containing PII.

8. The Partner certifies that it: (1) has reviewed all of the Commonwealth's Enterprise Information Security Policy (https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards); (2) will implement and maintain reasonably appropriate confidentiality and security procedures and practices necessary to protect personal information to which the Partner is given access through the RDC from the unauthorized access, destruction, use, modification, disclosure, or loss; and (3) will be responsible for the full or partial breach of any of these terms by its employees (whether such employees are direct or contracted) or subcontractors.

9. The Partner will not share PII with any other Provider Organizations or CoCs, except as authorized by the clients through a ROI.

10. If the Partner or DHCD receives from any entity a request to perform research using the RDC PII, all such requests must be referred to the RDC Administrator, and will be evaluated on a case by case basis with input from DHCD and the CoCs participating in the RDC.

11. The Partner will immediately notify DHCD in the event of any security breach including the unauthorized access, disbursement, use or disposal of PII, and in the event of a security breach the Partner will cooperate fully with DHCD, will provide access to any information necessary to respond to the security breach, and will be fully responsible for any damages and statutory, regulatory, or equitable penalties associated with the Partner's breach, including without limitation, those imposed pursuant to G.L. c. 66A, G.L. c. 93H, or G.L. c. 214, § 3B.

12. This agreement can be amended only upon the written agreement of the parties.

13. The Parties mutually agree that the following named individual is designated as the point of contact for RDC issues, and will be responsible for ensuring that the security and privacy arrangements specified in this Agreement are observed.

_____
Name

_____
CoC

_____
Street Address

_____
City/State/Zip Code

_____
Phone Number

_____
E-mail Address

The Parties mutually agree that the following named individual is designated as the point of contact for DHCD and will be responsible for ensuring that the security and privacy arrangements specified in this Agreement are observed.

[RDC Administrator]

_____
Name

_____
Title

_____
Street Address

_____
City/State/Zip Code

_____
Phone Number

_____
E-mail Address

14. The Partner will notify DHCD immediately of any changes in the organization's structure (merger, bankruptcy, etc.) or management, as well as changes to the Partner's contact person.

15. The persons executing this agreement on behalf of DHCD and the Partner represent and warrant that they are authorized to do so and to legally bind the organizations they represent to all the terms and provisions set forth herein.

CoC Lead Agency	**HMIS Lead Agency** (If different than CoC Lead Agency)
_____ Signature	_____ Signature
_____ Name (Printed)	_____ Name (Printed)
_____ Title	_____ Title
_____ CoC Lead Agency	_____ HMIS Lead Agency
_____ Date	_____ Date

Massachusetts Department of Housing and Community Development

_____
Signature

_____
Name (Printed)

_____
Title

_____
Date

Attachment 1

DEFINITIONS
The following terms as used in this document have the meanings ascribed to them below.

"Authorized Users" means employees of DHCD or Provider Organizations or others who have been approved by the RDC Administrator to access the information in the RDC.

"Client" means a homeless or at risk individual or group of individuals served by a Provider.

"CoC" or "Continuum of Care" means a planning group responsible for applying for federal homeless funs and developing data-driven strategies to address homelessness in a particular geographic area pursuant to 24 C.F.R. Part 578.

"CoC End User" means the CoC staff identified by each CoC as responsible for HUD and CoC reporting.

"Commonwealth" means the Commonwealth of Massachusetts.

"Coordinated Entry" means a centralized or coordinated process designed to coordinate program participant intake assessment and provision of referrals to, at a minimum, CoC and ESG programs within a CoC. A coordinated entry system covers the CoC's geographic area, is easily accessed by individuals and families seeking housing or services, includes a comprehensive and standardized assessment tool, and prioritizes those with the greatest needs.

"CSV" means Comma Separated Value file format.

"DHCD" means the Commonwealth of Massachusetts Executive Office of Housing and Economic Development Department of Housing and Community Development

"Drill Down" means a capability that will take the CoC End User from a more general view of the data to a more specific one at the click of a mouse. For example, CoC End Users will be able to click on a measure in a HUD Report and be brought to a list of individual Clients who are counted in that measure and the individual information specific to that measure.

"HMIS" means Homeless Management Information System.

"HMIS Data Dictionary" means the data dictionary designed for HMIS vendors and lead agency system administrators to identify the data elements required in an HMIS and understand the function and specific use of each element by the appropriate federal partner.
"HMIS Data Standards" means the HUD documentation of requirements for the programming and use of all HMIS systems and comparable database systems, effective October 1, 2019, including the HMIS Data Dictionary and the HMIS Data Standards Manual, as the same may be modified or amended. For more information see https://www.hudexchange.info/resource/3824/hmis-data-dictionary/.

"HMIS Data Standards Manual" means the standards manual that supports data collection and reporting efforts of HMIS Lead Agencies, CoCs, HMIS Lead Agencies, HMIS System Administrators, and HMIS

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" means the U.S. Department of Housing and Urban Development.

"PII" or "Personal Identifying Information" means personal information or data of a resident of the Commonwealth that is protected from disclosure under Federal and state privacy laws, including without limitation M.G.L. c. 66 and implementing regulations at 940 C.M.R. 11, M.G.L. c. 93H and implementing regulations at 201 C.M.R. 17, and HIPAA.

"Provider" or "Provider Organization" means an organization providing shelter and/or supportive services to Clients.

"Provider End User" means staff of participating Providers who are authorized to view Client PII when in receipt of an applicable ROI.

"RDC" or "Rehousing Data Collective" means the Rehousing Data Collective to be developed to provide access to integrated HMIS data on individuals and families across CoC boundaries in Massachusetts.

"RDC Administrator" means DHCD staff who are responsible for administering the RDC.

"RDC End User" means a party authorized to access the RDC with a user account and password for the purposes described in this document.

"RDC Uploader" means authorized staff with DHCD, CoCs, and certain authorized Providers who will be responsible for uploading HMIS datasets from their HMIS implementation into the RDC

"ROI" means a release of information signed by a Client (or, in the case of a Client Household, by the Client who has been identified as the head of household), authorizing access to the Client's PII as described in this RFQ.

Attachment 2

		DATA TYPE					
RDC END USER ROLE*	**RDC End User Role Definition**	**Full HMIS datasets with client PII**	**Full de-identified HMIS Datasets (hashed)**	**Federal reports w/ client PII reveled in "drill-downs"**	**Limited client PII for CE purposes, w/ ROI**	**Aggregate, de-identified reports for CoCs**	**Aggregate, de-identified reports**
RDC Administrator	DHCD staff who are responsible for administering the RDC	X	X	X	X	X	X
RDC Uploader	Authorized staff with DHCD, CoCs, and certain authorized Providers who will be responsible for uploading HMIS datasets from their HMIS implementation into the RDC	X (for datasets their org uploaded)		X (for datasets their org uploaded)			X
CoC End User	The CoC staff identified by each CoC as responsible for HUD and CoC reporting			X	X	X	X
Provider End User	Staff of participating Providers who are authorized to view Client PII when in receipt of an applicable ROI				X		X
Researcher	No RDC End User account will be provided to researchers, however they may access some data retrieved from the RDC for approved research projects	X (when CoCs have agreed)	X (when CoCs have agreed)				X
Public Interface User	A member of the public or a state agency other than DHCD, who has no RDC End User account, who will access aggregated reports and have limited ability to query the RDC based on de-identified datasets via a public-facing web interface.						X

*Note that Authorized Users can have multiple roles applied to their account. For example, in most CoCs the HMIS Lead would be responsible for both completing HMIS Dataset uploads to RDC as well as submitting CoC reports to HUD, and thus would have both the RDC Uploader and CoC End User roles applied to their RDC End User account.

10

Attachment 3

Data available in the Rehousing Data Collective

- 2.01 Organization Information
- 2.02 Project Information
- 2.03 Continuum of Care Information
- 3.01 Name
- 3.02 Social Security Number (only last 4 digits)
- 3.03 Date of Birth
- 3.06 Gender
- 3.07 Veteran Status
- 3.08 Disabling Condition
- 3.10 Project Start Date
- 3.11 Project End Date
- 3.12 Destination
- 3.16 Client Location
- 3.20 Housing Move-in Date
- 3.917 Living Situation
- 4.2 Income and Sources
- 4.3 Non Cash Benefits
- 4.12 Current Living Situation
- 4.14 Bed Night Date
- 4.19 Coordinated Entry Assessment
- 4.20 Coordinated Entry Event
- 4.43 Last Permanent Address
- 5.0x Metadata Elements (Date created, date updated, data collection stage, information date, project identifier, enrollment identifier, user identifier, personal identifier, household identifier)
- 5.8 Personal ID
- 5.9 Household ID

Timeline

Initially each CoC HMIS Lead will upload a full HMIS dataset with a start date of 10/1/2012, containing only projects that serve homeless or at-risk persons.

Thereafter, the Partner will upload full HMIS datasets on at minimum a monthly basis, with a start date of no less than one year prior.

APPENDIX 3: DESIGNATION OF AUTHORIZED SIGNATORY

ETO / ASIST DESIGNATION OF AUTHORIZED SIGNATORY

I, the undersigned, certify that I am the executive director, or other chief executive officer, of the below-named agency and that I have legal authority to sign legally binding documents on behalf of the below-named agency. I hereby designate the individual named below to complete all Site Administrative duties as described in the Participation Agreement between the Massachusetts Department of Housing and Community (DHCD) and the Agency signed on _____.

_____

Agency name

_____

Agency address

_____ _____

Signature of executive director or other chief executive officer

_____

Printed name and exact title of executive director or other chief executive officer

_____

Printed name and title of Site Administrator

Site Administrators' Phone: (____) _____-_____

Site Administrators' Fax: (____) _____-_____

Site Administrators' E-mail: _____

APPENDIX 4: ASIST USER REQUEST FORM

ASIST User Request Form

New User Information

Full Name: _____
Last *First* *M.I.*

Work Location: _____

Email Address: _____

Work Phone: _____

Title: _____

ETO ASIST Access Information

Site: _____

User Role: _____

Program Access:

1 _____
2 _____
3 _____
4 _____
5 _____

Site Administrator Authorization

Full Name: _____
Last *First* *M.I.*

Date: _____

Work Phone: _____

Instructions for filling out the ASIST User Request Form

*This form can only be filled out and submitted by the legal Site Administrator.

New User Information:

Fill out all fields. The e-mail address used should be the staff persons official work e-mail address, not a personal one.

ETO ASIST Access Information:

List the site in ETO ASIST that the user is being granted access to, their user role (see list below) and the program(s) that user should be granted access to.

User Roles from lowest to highest are:

- Intake
- Funders/Reports Only
- Staff
- Program Manager
- Department Head
- Site Administrator

Staff persons should be assigned the lowest user role necessary to do their job; for most users this will be either Staff or Program Manager.

Site Administrator Authorization:

The Site Administrator should fill out his or her own information in these fields. The request must come from the legal Site Administrator that DHCD has on file; if the Site Administrator has left the organization the Executive Director must fill out a new *ETO / ASIST Designation of Authorized Signatory* form appointing a new Site Administrator for the organization.

APPENDIX 5: AUTHORIZED USER LIST

Cape Cod and Islands CoC HMIS Authorized User List

CHO: _____

Date: _____

Person Submitting Form: _____

User Name: _____

User Name: _____

User Name: _____

User Name: _____

User Name: _____

User Name: _____

User Name: _____

User Name: _____

User Name: _____

User Name: _____

User Name: _____

This form must be completed and submitted every quarter to Martha Taylor, CoC Program Manager. Please email the form to martha.taylor@barnstablecounty.org. Make copies of the form if you need additional pages.

Quarterly due dates are January 15, April 15, July 15, October15

Agency HMIS Users not listed must have HMIS access removed by the CHO Site Administrator.

APPENDIX 6: DATA COLLECTION TEMPLATES – CLIENT DATA

CLIENT DATA TEMPLATE

FIRST NAME
MIDDLE NAME
LAST NAME
SUFFIX

- ☐ Jr.
- ☐ Sr.
- ☐ I
- ☐ II
- ☐ III
- ☐ IV

NAME DATA QUALITY

- ☐ Full name reported
- ☐ Partial name reported
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

GENDER

- ☐ Female
- ☐ Male
- ☐ Trans Male (FTM)
- ☐ Trans Female (MTF)
- ☐ Gender non-conforming
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

DATE OF BIRTH / /
DATE OF BIRTH DATA QUALITY

- ☐ Full DOB reported
- ☐ Partial DOB reported
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

SOC SEC # - -
SOC SEC DATA QUALITY

- ☐ Full DOB reported
- ☐ Partial DOB reported
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

AGENCY
STAFF CONTACT
PROJECT START DATE / /
PROJECT NAME
PROJECT TYPE

- ☐ Permanent Supportive Housing
- ☐ Rapid Re-Housing
- ☐ Transitional Housing
- ☐ Outreach
- ☐ Other Services Only (specify) _____
- ☐ Coordinated Entry
  - ☐ Individual
  - ☐ Family

PRIMARY LANGUAGE
INTERPRETER NEEDED?

- ☐ Yes
- ☐ No

ETHNICITY

- ☐ Hispanic/Latino
- ☐ Non-Hispanic/Latino
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

RACE

- ☐ American Indian/Native Alaskan
- ☐ Asian
- ☐ Black/African American
- ☐ Native Hawaiian/Pacific Islander
- ☐ White
- ☐ More than one
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

VETERAN STATUS (ADULTS ONLY)

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

APPENDIX 7: DATA COLLECTION TEMPLATES – PROJECT ENTRY ASSESSMENT

PROJECT ENTRY ASSESSMENT

CLIENT NAME (ALL ADULTS AND CHILDREN)

ASSESSMENT DATE (ALL ADULTS AND CHILDREN) ☐ / / ☐

MOVE-IN DATE (HEADS OF HOUSEHOLD) ☐ / / ☐

RELATIONSHIP TO HEAD OF HOUSEHOLD (ALL ADULTS AND CHILDREN)

- ☐ Self (HoH)
- ☐ HoH's child
- ☐ HoH's spouse or partner
- ☐ HoH's other relation
- ☐ Other: non-relation

PRIOR LIVING SITUATION - [1] RESIDENCE PRIOR TO PROJECT ENTRY (ALL ADULTS)

HOMELESS SITUATION
- ☐ Emergency shelter, including hotel or motel paid for with ES voucher
- ☐ Place not meant for habitation
- ☐ Safe Haven

INSTITUTIONAL SITUATION
- ☐ Foster care
- ☐ Hospital or other non-psychiatric medicaal facility
- ☐ Jail, prison, or juvenile detention facility
- ☐ Long-term care or nursing home
- ☐ Psychiatric hospital
- ☐ Substance abuse facility or detox

TRANSITIONAL AND PERMANENT HOUSING SITUATION
- ☐ Hotel or motel, no emergency shelter voucher
- ☐ Owned by client, no subsidy
- ☐ Owned by client, with subsidy
- ☐ Permanent housing (other than RRH) for formerly homeless persons
- ☐ Rental by client, no subsidy
- ☐ Rental by client, VASH
- ☐ Rental by client, GPD TIP
- ☐ Rental by client, other subsidy (including RRH)
- ☐ Residential project or halfway house with no homeless criteria
- ☐ With family
- ☐ With friends
- ☐ Transitiional Housing
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected
- ☐ Host Home (non-crisis)
- ☐ Rental by client with HCV (tenant or project-based)
- ☐ Rental by client in a public housing unit

DATE HOMELESSNESS STARTED (ALL ADULTS)

☐ / / ☐

[2] LENGTH OF STAY IN PRIOR LIVING SITUATION (ALL ADULTS)
- ☐ One night or less
- ☐ Two to six nights (7 days)
- ☐ One week or more, but less than one month
- ☐ One month or more, but less than 90 days
- ☐ 90 days or more, but less than one year
- ☐ One year or longer
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

[3] NUMBER OF EPISODES OF HOMELESSNESS (STAYING IN EMERGENCY SHELTER OR IN A PLACE NOT MEANT FOR HABITATION) CLIENT HAS EXPERIENCED OVER THE PAST 3 YEARS (ALL ADULTS)
- ☐ 1 time
- ☐ 2 times
- ☐ 3 times
- ☐ 4 or more times
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

[4] TOTAL NUMBER OF MONTHS HOMELESS (STAYING IN EMERGENCY SHELTER OR IN A PLACE NOT MEANT FOR HABITATION) IN THE PAST 3 YEARS (ALL ADULTS)
- ☐ 1 month
- ☐ 2 months
- ☐ 3 months
- ☐ 4 months
- ☐ 5 months
- ☐ 6 months
- ☐ 7 months
- ☐ 8 months
- ☐ 9 months
- ☐ 10 months
- ☐ 11 months
- ☐ 12 months
- ☐ More than 12 months
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

IS THE CLIENT CURRENTLY RECEIVING INCOME FROM ANY SOURCE? (ALL ADULTS)

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

IF YES, CHECK AS MANY AS APPLY - INCLUDE MONTHLY AMOUNT

☐	Earned income (employment)	$	☐	VA Non-service Connected Disability	$	☐	SS Retirement	$
☐	Unemployment Insurance	$	☐	Private Disabillity	$	☐	Pension	$
☐	SSI	$	☐	Worker's Comp	$	☐	Child support	$
☐	SSDI	$	☐	TANF	$	☐	Alimony or other spousal support	$
☐	VA Service-Connected Disability	$	☐	General Assistance	$	☐	Other (specify)	$

IS THE CLIENT CURRENTLY RECEIVING NON-CASH BENEFITS FROM ANY SOURCE? (ALL ADULTS)

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

If YES, check as many as apply:

- ☐ SNAP
- ☐ WIC
- ☐ TANF Child Care
- ☐ TANF Transportation
- ☐ Other TANF Services
- ☐ Other (specify) _____

IS THE CLIENT CURRENTLY COVERED BY HEALTH INSURANCE? (ALL ADULTS AND CHILDREN)

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

If YES, check as many as apply:

- ☐ Medicaid (MASSHEALTH, etc.)
- ☐ Medicare
- ☐ State Children's Health Insurance
- ☐ VA Medical Services
- ☐ Employer provided
- ☐ COBRA
- ☐ Private pay
- ☐ State Health Isurance for Adults (this is NOT MASSHEALTH)
- ☐ Indian Health Services Program
- ☐ Other (specify) _____

HEALTH INFORMATION (ALL ADULTS AND CHILDREN)

DOES CLIENT CURRENTLY HAVE A DISABLING CONDITION

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

DOES CLIENT HAVE A *DEVELOPMENTAL DISABILITY*

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

DOES THE CLIENT HAVE *HIV/AIDS*

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

DOES CLIENT HAVE A *PHYSICAL DISABILITY*

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

If YES, is the client's physical disability expected to be of long–continued and indefinite duration and substantially impairs ability to live independently?

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

DOES CLIENT HAVE A *CHRONIC HEALTH CONDITION*

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

If YES, is the client's condition expected to be of long–continued and indefinite duration and substantially impairs ability to live independently?

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

DOES THE CLIENT HAVE A *SUBSTANCE ABUSE PROBLEM*

- ☐ No
- ☐ Alcohol
- ☐ Drugs
- ☐ Both Alcohol and Drugs
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

DOES CLIENT HAVE A *MENTAL HEALTH PROBLEM*

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

If YES, is the client's mental health problem expected to be of long–continued and indefinite duration and substantially impairs ability to live independently?

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

IS CLIENT A VICTIM / SURVIVOR OF DOMESTIC VIOLENCE (ALL ADULTS)

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

IF YES, WHEN DID THE LAST EPISODE OCCUR?

- ☐ Within past 3 months
- ☐ 3 - 6 months
- ☐ 6 months - 1 year
- ☐ One year or more
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

IS CLIENT CURRENTLY FLEEING DOMESTIC VIOLENCE?

- ☐ Yes
- ☐ No
- ☐ Client doesn't know
- ☐ Client refused
- ☐ Data not collected

APPENDIX 8: DATA COLLECTION TEMPLATES – ANNUAL / UPDATE ASSESSMENT

PROJECT ANNUAL ASSESSMENT / UPDATE ASSESSMENT

CLIENT NAME	
PROJECT NAME	
ASSESSMENT DATE	/ /
ASSESSMENT TYPE	ANNUAL UPDATE

IS THE CLIENT CURRENTLY COVERED BY HEALTH INSURANCE (ALL ADULTS AND CHILDREN)

- ☐ Yes
- ☐ No
- ☐ Client Doesn't Know
- ☐ Client Refused

If YES, check as many as apply:

- ☐ Medicaid
- ☐ Medicare
- ☐ State Children's Health Insurance Program
- ☐ VA Medical Services
- ☐ Employer-Provided Health Insurance
- ☐ COBRA
- ☐ Private Pay
- ☐ State Health Insurance For Adults
- ☐ Indian Health Services Program
- ☐ Other (specify) _____

HAS CLIENT BECOME DISABLED OR BEEN DIAGNOSED WITH AND ADDITIONAL DISABILITY SINCE ENROLLING IN PROJECT (ALL ADULTS AND CHILDREN)

- ☐ Yes
- ☐ No
- ☐ Client Doesn't Know
- ☐ Client Refused

If YES, check as many as apply:

- ☐ Chronic health condition
- ☐ Developmental disability
- ☐ HIV/AIDS
- ☐ Mental health disability
- ☐ Physical disability
- ☐ Substance abuse
  - ☐ Drugs
  - ☐ Alcohol
  - ☐ Both drugs and alcohol

DOES THE CLIENT HAVE CASH INCOME FROM ANY SOURCE (ALL ADULTS)

- ☐ Yes
- ☐ No
- ☐ Client Doesn't Know
- ☐ Client Refused

If YES, check as many as apply:

	Monthly amount:
☐ Earned income (employment)	$
☐ Unemployment Insurance	$
☐ SSI	$
☐ SSDI	$
☐ VA Disability	$
☐ Private Disabillity	$
☐ Worker's Comp	$
☐ TANF	$
☐ General Assistance	$
☐ SS Retirement	$
☐ Pension	$
☐ Child support	$
☐ Alimony or other spousal support	$
☐ Other (specify) _____	$

DOES THE CLIENT HAVE NON-CASH BENEFITS FROM ANY SOURCE (ALL ADULTS)

- ☐ SNAP
- ☐ WIC
- ☐ TANF Child Care
- ☐ TANF Transportation
- ☐ Other TANF Services
- ☐ Section 8 or other rental assistance
- ☐ Temporary rental assistance
- ☐ Other (specify) _____

APPENDIX 9: DATA COLLECTION TEMPLATES – EXIT ASSESSMENT

PROJECT EXIT ASSESSMENT

CLIENT NAME
PROJECT NAME
ASSESSMENT DATE ____/____/____

HAS PARTICIPANT BEEN DISMISSED FROM PROJECT?

☐ YES ☐ NO

QUESTIONS FOR ALL ADULTS AND CHILDREN

WHERE WILL CLIENT BE STAYING IMMEDIATELY AFTER LEAVING THIS PROJECT

- ☐ Deceased
- ☐ Emergency Shelter, including hotel/motel with ES voucher
- ☐ Foster care
- ☐ Hospital or other residential non-psychiatric medical facility
- ☐ Hotel/motel without ES voucher
- ☐ Jail, prison, or juvenile detention
- ☐ Long-term care or nursing home
- ☐ Moved from one HOPWA funded project to HOPWA PH
- ☐ Moved from one HOPWA funded project to HOPWA TH
- ☐ Owned by client, no ongoing housing subsidy
- ☐ Owned by client, with ongoing housing subsidy
- ☐ Permanent housing for formerly homeless persons (such as CoC project)
- ☐ Place not meant for habitation (return to homelessness)
- ☐ Psychiatric hospital or other psychiatric facility
- ☐ Rental by client, no ongoing subsidy
- ☐ Rental by client, with VASH subsidy
- ☐ Rental by client, with GPD TIP subsidy
- ☐ Rental by client, with other ongoing subsidy
- ☐ Safe Haven
- ☐ Staying with family (permanent)
- ☐ Staying with family (temporary)
- ☐ Staying with friends (permanent)
- ☐ Staying with friends (temporary)
- ☐ Substance abuse treatment facility or detox center
- ☐ Transitional housing for homeless persons (including homeless youth)
- ☐ Other (describe):_____
- ☐ No exit interview completed
- ☐ Client doesn't know
- ☐ Client refused

IS CLIENT STILL /CURRENTLY COVERED BY HEALTH INSURANCE

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

(Answer YES or NO for each source - answer NO for sources that have been terminated, even if they were received in the past

NO	YES	
☐	☐	Medicaid
☐	☐	Medicare
☐	☐	State Children's Health Insurance Program
☐	☐	VA Medical Services
☐	☐	Employer-Provided Health Insurance
☐	☐	COBRA
☐	☐	Private Pay
☐	☐	State Health Insurance For Adults
☐	☐	Indian Health Services Program
☐	☐	Other (specify) _____

PHYSICAL DISABILITY - Does the client currently have a PHYSICAL DISABILITY?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

If YES: Is the disability expected to be long-term and impair client's ability to live independently

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is documentation of the the disability and severity on file?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is the client currently receiving services/treatment for this disability?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

CHRONIC HEALTH CONDITION - Does the client currently have a CHRONIC HEALTH CONDITION

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

If YES: Is the condition expected to be long-term and impair client's ability to live INDEPENDENTLY

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is documentation of the condition and severity on file?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is the client currently receiving services/treatment for this condition?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

DEVELOPMENTAL DISABILITY - Does the client currently have a DEVELOPMENTAL DISABILITY?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

If YES: Is the disability expected to be long-term and impair client's ability to live independently?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is documentation of the the disability and severity on file?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is the client currently receiving services/treatment for this disability?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

HIV/AIDS - Does the client currently have HIV/AIDS?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

If YES: Is HIV/AIDS expected to be long-term and impair client's ability to live independently?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is documentation of HIV/AIDS and severity on file?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is the client currently receiving services/treatment for HIV/AIDS?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

MENTAL HEALTH PROBLEM - Does the client currently have a MENTAL HEALTH PROBLEM?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

If YE Is the mental health problem expected to be long-term and impair client's ability to live independently?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is documentation of the mental health problem and severity on file?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is the client currently receiving services/treatment for this mental health problem?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

SUBSTANCE ABUSE PROBLEM - Does the client currently have a SUBSTANCE ABUSE PROBLEM?

☐ Alcohol abuse ☐ No
☐ Drug abuse ☐ Client Doesn't Know
☐ Both alcohol and drug ☐ Client Refused

If Yes: Is the substance abuse problem expected to be long-term and impair client's ability to live independently

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is documentation of the substance abuse problem and severity on file?

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Is the client currently receiving services/treatment for this substance abuse abuse problem

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

DOES CLIENT HAVE CASH INCOME FROM ANY SOURCE (ALL ADULTS)

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

If YES, select all that apply:

		Monthly amount:
☐	Earned income (employment)	$
☐	Unemployment Insurance	$
☐	SSI	$
☐	SSDI	$
☐	VA Disability	$
☐	Private Disabillity	$
☐	Worker's Comp	$
☐	TANF	$
☐	General Assistance	$
☐	SS Retirement	$
☐	Pension	$
☐	Child support	$
☐	Alimony or other spousal support	$
☐	Other (specify)	$

DOES CLIENT HAVE NON-CASH BENEFITS FROM ANY SOURCE (ALL ADULTS)

☐ Yes ☐ Client Doesn't Know
☐ No ☐ Client Refused

Answer YES or NO for each non-cash benefit source. Answer NO for benefits that have been terminated, even if they were received in the past.

NO	YES	
☐	☐	SNAP
☐	☐	WIC
☐	☐	TANF Child Care
☐	☐	TANF Transportation
☐	☐	Other TANF Services
☐	☐	Section 8 or other rental assistance
☐	☐	Temporary rental assistance
☐	☐	Other (specify)

APPENDIX 10: DATA QUALITY BENCHMARKS

General Principle	Specific Principle	Expected Benchmark	Monitoring Procedure Who? How often?
Coverage	All lodging and non- lodging homeless programs in the CoC report HMIS data	- 100% Emergency shelter beds and Rapid Rehousing beds report in HMIS - 80% Transitional housing and permanent supportive housing report in HMIS.	- HIC provides annual report. - HMIS Administrator reports status quarterly to HMIS Committee.
Completeness	All clients entered	- 95% of clients have all universal data entered. - 95% of clients have project entry assessment completed. - 100% of clients qualifying for Annual assessment must have assessment completed.	- HMIS Administrator runs monthly Data Validation reports and sends to CHOs for data clean up.
	Complete exit data entered	- 95% of required exit assessments entered. - 95% of exits assessments contain complete exit information, including Exit Destination	- HMIS Administrator checks missing exit assessments and missing exit destinations on monthly Data Validation report.
Accuracy	Accurate data entered by staff	- 5 of the 6 records must be entered accurately.	- Annual random spot check of CHO paper files by HMIS Administrator against HMIS. Pull 6 records and look for client data in the database.
Timeliness	Changing data kept up to date	- Active clients should be reviewed by the local database administrator every 30 days.	- The HMIS Administrator will review with the CHO Site Administrator on quartery basis.
	Data are entered soon after collected	- Emergency Shelter clients must be entered within 24 hours of intake. - All non-Emergency Shelter clients must be entered within 48 hours of intake.	- If unable to must inform the CHO executive director and HMIS Administrator by email the reason unable to do so and the clients ID. Monthly reports to agencies in person or via Go to Meeting.
Consistency	Common interpretation of questions and answers	- Data will be reviewed at the monthly data management meetings.	- The HMIS Administrator will compare aggregate data by users for same population to look for unusual patterns on a quarterly basis. - Inconsistencies found during the month will be noted and discussed at data management meetings.
	Common knowledge of what fields to answer	- 95% of required fields completed	- Monthly check of required fields in system – 95% of records have complete minimal fields.

APPENDIX 11: IDENTIFICATION OF SECURITY OFFICER

Identification of Security Officer

Organization Name

Security Officer Name

Title

Phone

Email

Security Officer duties include, but are not limited to:

- Annually review the Security Certification document and test the CHO security practices for compliance.
- Using this Security Certification document, certify that the CHO adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time. Communicate any security questions, requests, or security breaches to the Cape Cod and Islands HMIS System Lead and Security Officer.
- Communicate security related HMIS information to the organization's end users.
- Complete security training offered by the HMIS Lead.
- Additional duties specified in the HMIS Participation Agreement.

CHO Security Officer signature indicating understanding and acceptance of these duties:

_____

Signature Date

APPENDIX 12: SECURITY COMPLIANCE CERTIFICATION

Category	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
User Authentication	Does the agency abide by the HMIS policies for unique usernames and password?	All HMIS users at the agency are aware that they should: _____Y_____N - NEVER share username and passwords _____Y_____N - NEVER keep usernames/ passwords in public locations _____Y_____N - NEVER use their internet browser to store passwords	
Hard Copy Data	Does agency have procedures in place to protect hard copy PII (PPI) generated from or for the HMIS?	Agency has procedure for hard copy PII that includes: Security of hard copy files: _____Y_____N - Locked drawer/file cabinet _____Y_____N - Locked office Procedure for client data generated from the HMIS: _____Y_____N - Printed screen shots _____Y_____N - HMIS client reports _____Y_____N - Downloaded data into Excel	
Storage	Does the agency dispose of or remove identifiers from a client record after a specified period of time? (Minimum standard: 7 years after PII was last changed if record is not in current use.)	_____Y_____N - Agency has a procedure Describe procedure: _____ _____ _____	

Virus Protection	Do all computers have virus protection with automatic update? (This includes non-HMIS computers if they are networked with HMIS computers.)	Virus software and version _____ _____Y_____N - Auto-update turned on	
Firewall	Does the agency have a firewall on the network and/or workstation(s) to protect the HMIS systems from outside intrusion?	Single computer agencies: _____Y_____N - Individual workstation Version: _____ Networked (multiple computer) agencies: _____Y_____N - Network firewall	
Physical Access	Are all HMIS workstations in secure locations or are they manned at all times if they are in publicly accessible locations? (This includes non-HMIS computers if they are networked with HMIS computers.)	All workstations are: _____Y_____N - In secure locations (locked offices) or manned at all times _____Y_____N - Using password protected screensavers All printers used to print hard copies from the HMIS are: _____Y_____N - In secure locations	
Data Disposal	Does the agency have policies and procedures to dispose of hard copy PII or electronic media?	_____Y_____N - Agency shreds all hardcopy PII before disposal Before disposal, the Agency reformats/degausses (demagnetizes): _____Y_____N - Discs _____Y_____N - CDs _____Y_____N - Computer hard-drives _____Y_____N - Other media (tapes, jump drives, etc.)	

Software Security	Do all HMIS workstations have current operating system and internet browser security? (This includes non-HMIS computers if networked with HMIS computers.)	Operating System (OS) Version: _____ _____ _____Y_____N - All OS updates are installed _____Y_____N - Most recent version of Internet Browser(s) is installed	

SECURITY COMPLIANCE SELF-CERTIFICATION

We affirm and certify the above information is true and that this organization, _____, is in full compliance with all requirements listed as "CHO" (Covered Homeless Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the Cape and Islands CoC HMIS Policies and Procedures or will be in compliance within the timeframes stated above. This certification is incorporated into the HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

HMIS Security Contact Signature: _____

Date: _____

Executing Officer Signature: _____

Date: _____

APPENDIX 13: DATA COLLECTION NOTICE

Data Collection Notice

We collect personal information directly from you for reasons that are discussed in our privacy statement.

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 is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons.

We only collect information that we consider to be appropriate.

Recopilación de Datos

Recopilamos información personal directamente de usted por las razones que se discuten en nuestra declaración de privacidad.

Podemos ser requeridos recopilar alguna información personal por ley o por las organizaciones que nos dan dinero para operar este programa. Otra información personal que recopilamos es importante para ejecutar nuestros programas, mejorar los servicios para las personas sin hogar, y para comprender mejor las necesidades de las personas sin hogar.

Nosotros solamente recopilamos información que consideramos apropiado.

APPENDIX 14: PRIVACY NOTICE - ENGLISH

Cape Cod and Islands CoC HMIS Privacy Notice

This notice describes how we may use and share information we have about you and how you can access that information.

HMIS is a database that stores information about clients we serve and services we provide. We collect information that is defined in the U.S. Department of Housing and Urban Development's HMIS Data Standards. This notice applies to the Cape Cod and Islands CoC HMIS system.

Uses and Disclosures of Your Information

Information you provide…

- Will be entered into the Cape Cod and Islands CoC HMIS database known as ETO.
- Will be used to improve, provide and coordinate services.
- May be used in relation to payment or reimbursement for services.
- Will be used to make sure that our programs are effective.
- Will be used to prepare statistical reports, but only aggregate data will be provided to funders, media, or any state or local agency. No social security numbers, Date of birth or names will be released without your written consent and consent between the sender and receiver of the information. You may revoke this consent at any time.

Information you provide about physical or mental health problems will not be shared with other service providers unless you have authorized it.

Protected Identifiable Information (PII) will be shared only if you authorize it or if required by law, or if there is a serious threat to health or safety.

In Massachusetts, PII includes your name, date of birth, social security number, driver's license number, and bank account numbers. We **DO NOT** collect driver's license or bank account numbers.

Your Rights

- Your right to receive services will not be affected if you refuse to provide HMIS information.
- You control who your information is shared with. You may allow or refuse to share your information with other service providers.

- You may give written notice to end all privacy and information sharing agreements at any time.
- You may have a copy of this notice.
- You may view your record, have your record corrected, and file a complaint.

How to Inspect and Correct Your Personal Information

You may request a copy of your HMIS record. Please submit a verbal or written request to program staff to get a copy. We will explain any information on it that you do not understand.

We will consider your request to correct inaccurate or incomplete personal information. We may delete or fix information that we agree is inaccurate or incomplete.

We may deny your request to inspect your personal information if…

- The information was gathered in reasonable anticipation of legal actions.
- The information would violate a confidentiality agreement.
- Sharing the information would endanger the life or safety of any individual.

If we deny your request, we will explain the reason. We will keep a record of the request and the reason it was denied.

Data Storage and Disposal

We dispose of personal information that is not being used **seven** years after it was created or updated. We may remove personal identifiers from the information instead of getting rid of it.

We may keep information longer if required by laws, statutes, regulations or contracts.

For more information contact the supervisor of your program.
To file a complaint, contact the Cape Cod and Islands HMIS lead:

Martha Taylor
Barnstable County Department of Human Services
P.O. Box 427
Barnstable, MA 02630
(508) 375-6625
martha.taylor@barnstablecounty.org

We have the right to change this notice at any time and changes may apply to information collected prior to the date of the change.
We accept and consider all questions or complaints regarding the Cape Cod and Islands Continuum of Care HMIS.

APPENDIX 15: PRIVACY NOTICE - SPANISH

HMIS del Condado de Cape Cod and Islands Notificacion de Privacidad

Este aviso describe como podemos utilizar t compartir la información que tenemos sobre usted y como usted puede tener acceso a esa información.

HMIS es una base de datos que almacena información acerca de los clientes que servimos y servicios que ofrecemos. Recopilamos la información que se define en el Departamento de Vivienda y Estándares de Datos HMIS de Desarrollo Urbano del EE. UU.. Este aviso se aplica al HMIS del Condado de Cape Cod and Islands.

Usos y Divulgaciones de su información

La información que usted proporcione…

- Se introducirá en el HMIS del Condado de Cape Cod and Islands.
- Se utilizará para mejorar, proveer y coordinar servicios.
- Puede ser utilizado en relación con el pago o rembolso de los servicios.
- Se utilizará para asegurar que nuestros programas sean eficaces.
- Se utilizará para preparar informes estadísticos.

La información que usted proporciona acerca de problemas de salud física o mental no será compartida con otros proveedores de servicios, a menos que usted haya autorizado.

Información de identificación protegida (PII) será compartida solo si usted lo autorice, o si lo requiere la ley, o si hay una amenaza seria a la salud o la seguridad.

En Massachusetts, PII incluye su nombre, fecha de nacimiento, numero de seguro social, numero de licencia de conducir y números de cuentas bancarias. No recopilamos números de licencia de conducir o cuentas bancarias.

Sus Derechos

- Su derecho a recibir los servicios no se vera afectado si se niega a proporcionar información de HMIS.
- Usted controla con quien su información se comparte. Puede permitir o denegar compartir su información con otros proveedores de servicios.
- Puede dar aviso por escrito para terminar los acuerdos del intercambio de información y privacidad en cualquier momento.
- Puedes obtener una copia de este aviso.
- Usted puede ver su expediente, tener su expediente corregido, y someter una queja.

Como revisar y corregir su información personal

Usted puede solicitar una copia de su expediente HMIS. Por favor, envié una solicitud verbal o por escrito al personal del programa para obtener una copia. Explicaremos cualquiera información que no entiende.

Consideraremos su solicitud para corregir la información personal que este inexacta o incompleta. Podemos eliminar o corregir la información en que estemos de acuerdo ser inexacta o incompleta.

Podemos negar su solicitud para revisar su información personal si...

- La información se recopilo en anticipación razonable de acciones legales.
- La información violaría un acuerdo de confidencialidad.
- Compartir la información pondría en peligro la vida o seguridad de cualquier persona.

Si negamos su petición le explicaremos la razón. Vamos a mantener un registro de la solicitud y la razón por la que fue denegada.

Almacenamiento de Datos y Eliminación

Disponemos información personal que no esta siendo utilizado siete anos después de su creación o actualización. Podemos quitar los identificadores personales de la información en lugar de deshacerse de ella.

Podemos mantener la información por más tiempo si lo requieren las leyes, estatutos, reglamentos o contratos.

Para mas información póngase en contacto con el supervisor de su programa.
Para someter una queja, comuníquese con La Continuidad de Cuidado del Condado De Cape Cod and Islands.

Martha Taylor
Barnstable County Department of Human Services
P.O. Box 427
Barnstable, MA 02630
(508) 375-6625
martha.taylor@barnstablecounty.org

We have the right to change this notice at any time and changes may apply to information collected prior to the date of the change.
We accept and consider all questions or complaints regarding the Cape Cod and Islands Continuum of Care HMIS.