Continuum of Care (CoC)

Homeless Management Information System (HMIS)

BostonHMIS
Policy and Procedure Manual

City of Boston
Mayor's Office of Housing
12 Channel Street, 905
Boston, MA 02210

CONTENTS

1. OVERVIEW

The BostonHMIS Standard Operating Procedures (SOP) documents the policies and procedures of the Homeless Management Information System (HMIS) on behalf of the Boston Continuum of Care. The purpose of this document is to help the HMIS Lead agency carry out routine HMIS operations. The SOPs aim to achieve efficiency, quality output, and uniformity of performance while reducing miscommunication and failure to comply with industry regulations. As appropriate, step-by-step instructions for the efficient, effective, and transparent operations are included. All HMIS Users and Covered/ Contributory Homeless Organizations (CHOs) must be provided a copy and be familiar with this document. For reference on terminology, refer to Section XX.

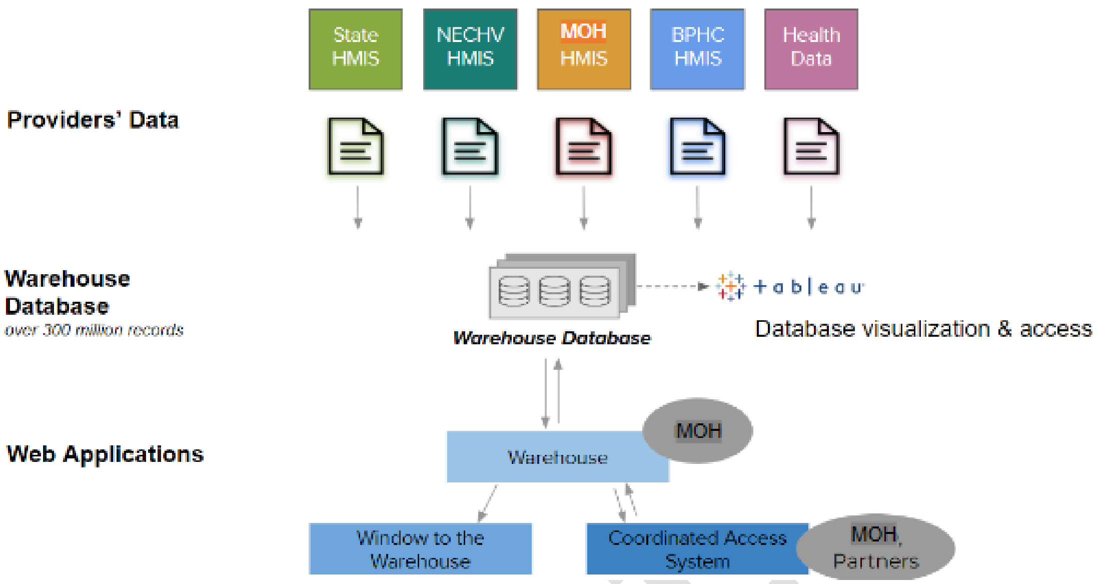
A document matrix is included in Appendix X. The matrix includes policy relevance to the various data systems contributing data to BostonHMIS and a version history of all changes and approvals to this document.

I. The Boston HMIS Data Structure

The BostonHMIS System consists of numerous software applications that collect, report, and contribute data to the BostonHMIS Data Warehouse. The BostonHMIS Data Warehouse is the Boston CoC's designated HMIS (Hereafter referred to as "BostonHMIS" or "the HMIS"). The City of Boston, Mayor's Office of Housing, as the CoC's designated HMIS Lead agency, also maintains and supports an optional HUD-compliant HMIS software application (front-end HMIS) titled "Clarity Human Services", which supports the use and operations of the BostonHMIS Data Warehouse. The Mayor's Office of housing as the funder of programs also reserves the right to require the usage of Clarity for certain funded programs.

Term	Description
BostonHMIS System	All CoC Data Systems, including warehouse
BostonHMIS or the HMIS	The BostonHMIS Data Warehouse. This is the CoC's designated HMIS
BostonHMIS Clarity or Clarity Human Services (Bitfocus)	Current optional software selected and managed by HMIS Lead (MoH)
Agency Managed or other HMIS applications	All other data systems managed by agencies or the state that contribute data to the data warehouse

Data comes to Boston in different forms and at different times.



Support of Agency Managed or other HMIS applications other than Clarity HMIS, are outside the scope of the HMIS Lead, however, **policies and procedures that apply to Clarity and the Data Warehouse will also apply to all software applications collecting, reporting, and contributing data to the BostonHMIS**. It is the expectation that all software and their management organizations will adhere to the HMIS Policies and Procedures outlined in this document. Agencies managing their own software may impose stricter policies and procedures than outlined in this document; however, they must not limit the collection, access, and contribution of data to the BostonHMIS (the Boston Data Warehouse).

2. Governance Structure

POLICY

HMIS shall be governed by the primary decision-making body of the Continuum of Care (CoC). The Mayor's Office of Housing (MOH), City of Boston, is designated as the CoC's HMIS Lead agency, under agreement with the general membership of the Boston Continuum of Care and authority of the Boston CoC Board. The HMIS Lead Agency guides the implementation of the HMIS. However, the CoC Board is ultimately responsible for the HMIS. The CoC Board ensures the participation of all qualified agencies in the BostonHMIS. The HMIS Lead Agency ensures HMIS Participation Agreements are executed with all qualified Contributory HMIS Organizations (CHO). The CoC ensures that the HMIS is being carried out according to the guidelines set forth in this document and the HMIS Data and Technical Standards provided by the U.S. Department of Housing and Urban Development (HUD). The HMIS Lead agency is also bound to data collection practices and requirements outlined in the current HMIS Data Standards, the HMIS Data Standards Manual, and the 2004 HMIS Technical Standards.[1]

PROCEDURE

The CoC's HMIS Lead Agency shall be responsible for the Organization and Management of BostonHMIS described below. An HMIS Lead Evaluation should be conducted annually to ensure adherence to HUD's HMIS Lead Standards and CoC requirements.

[1] HUD HMIS Landing Page

3. Participation Requirements

I. Participation Requirements

POLICY

A recipient, sub-recipient, project sponsor, or third-party partner must ensure that data on all persons served, and all activities provided are entered into an HMIS software application for the geographic area in which those persons and activities are located, or a comparable database, as provided under 24 CFR part 580. The entry, storage, and use of this data are subject to the HMIS requirements at 24 CFR part 580.

PROCEDURE

Any Participating Agency, mandatory or voluntary, is responsible for ensuring that a minimum set of data elements, referred to as the HUD Universal Data Elements (UDEs) as defined by the most current HUD HMIS Data Standards, are collected and/or verified from all clients at their initial program enrollment, or as soon as possible thereafter (with the exception of those serving domestic violence survivors). Participating Agencies must report client-level detail in the "Required Response Categories" for the UDEs that are shown in the most current HUD HMIS Data Standards.

Participating Agencies must enter into and stay in compliance with an HMIS Participation Agreement and must ensure that all end users have signed and are in compliance with HMIS End User Agreements.

II. Mandated Participation

POLICY

All designated agencies that are funded to provide homeless services by the City of Boston, State of Massachusetts Department of Health and Human Services (DHCD), Office of Child and Family Services (OFCS), Runaway and Homeless Youth (RHY), Projects for Assistance in Transition from Homelessness (PATH), Supportive Services for Veteran Families (SSVF), Veterans Affairs Supportive Housing (VASH) and/or HUD, must meet the minimum BostonHMIS participation standards as defined by this Policy and Procedures Manual. The proposed HUD Rule found at

24 CFR Parts 91, detailing HMIS Requirements states; “With respect to scope, this rule clarifies that all recipients of financial assistance under the Continuum of Care program, the Emergency Solutions Grant program, the Rural Housing Stability Assistance (RHS) program, as well as HUD programs previously funded under the McKinney-Vento Act (the Supportive Housing Program, the Shelter Plus Care program, and the Section 8 Single Room Occupancy Moderate Rehabilitation program) are required to use HMIS to collect client-level data on persons served.”

Victims Service Providers (VSPs) must maintain and use an HMIS-comparable database that meets all requirements of the HEARTH Act of 2009, the ESG Interim Rule, the CoC Interim Rule, and all associated guidance, including the HMIS Data Standards, HMIS Data Dictionary, HMIS Data Manual, and any publicly available guidance provided by HUD or its federal partners.

PROCEDURE

TBD-Correlate to monitoring procedures from MOH SHD DO Team.

III. Voluntary Participation

POLICY

BostonHMIS cannot require non-funded providers to participate in the BostonHMIS, however, they do work closely with non-funded agencies to articulate the benefits of HMIS, and to strongly encourage their participation. Full participation in the BostonHMIS ensures a comprehensive and accurate understanding of homelessness in the City of Boston and across the Commonwealth of Massachusetts.

PROCEDURE

Non-funded agencies may voluntarily agree to participate but will need to meet minimum participation standards however these agencies must already have a software system compatible with HMIS. BostonHMIS does not have the software licenses to support non-funded agencies.

IV. Partner Agency Agreements

POLICY

All agencies that contribute data to the Warehouse, regardless of the chosen front-end HMIS data applications, are required to sign the Boston Continuum of Care Homeless Management Information System Participation Agreement. This agreement spells out the expectations of MOH for the Agency in regard to data collection, data transfer processes, client privacy and confidentiality, network security, and interagency data sharing.

PURPOSE

To ensure clarity of roles and responsibilities and compliance with HMIS policies and procedures, agencies who access Clarity HMIS for any reason or who contribute data to the Warehouse must sign an enforceable agreement before any end-user access to either system.

PROCEDURE

Partner agencies signed an initial participation agreement upon first onboarding to the system. Additionally, the HMIS Participation Agreement is an attachment to MoH funded projects and contracts. For new agencies requesting access to Clarity HMIS, this Agreement will be part of the onboarding process once a request for access has been submitted.

VI. HMIS End-User Agreements

POLICY

All BostonHMIS users will execute an end-user agreement to access BostonHMIS.

PROCEDURE

Clarity

Clarity Users will sign, the end user agreement during initial login. The form will load and must be signed by the end user. Training related to the conditions in the end user agreement is provided in the LMS prior to the user gaining access to HMIS. End-user agreements expire annually and will be presented to the end user for signature upon expiration.

Boston HMIS Data Warehouse

A Boston CoC Help Desk Case must be submitted requesting Warehouse access for the user by an Authorized Submitter. All new users must complete training in the LMS prior to signing the end user agreement and being approved for access

ETO Software Systems

EA and Agency Managed ETO Software Systems should have a process in place to ensure that end-users are aware of the security, privacy, and confidentiality requirements of access to the system and a way maintain these end-user agreements.

Comparable Databases

Agency Managed Comparable databases should have a process in place to ensure that end-users are aware of the security, privacy, and confidentiality requirements of access to the system and a way maintain these end-user agreements.

VII. HMIS Policy Violations and non-compliance

POLICY

HMIS Users and Contributory Homeless Organizations (CHOs) must abide by all HMIS operational policies and procedures found in the BostonHMIS Policies and Procedures manual, Agency Agreement, and End User Agreement. Repercussion for any violation will be assessed in a tiered manner. Each User or CHO violation will face successive consequences – the violations do not need to be of the same type in order to be considered second or third violations. HMIS staff from the CoC's Lead Agency will determine the level of infraction. User violations do not expire. No regard is given to the duration of time that occurs between successive violations of the HMIS policies and procedures as it relates to corrective action. Violations of these policies and procedures will have potential negative impacts on an agency's ability to maintain CoC support for future funding opportunities (e.g. ESG and CoC/HUD funding).

PROCEDURE

Updates to policies and procedures will be documented and all users will be kept informed of changes by email. The most recent version of this document will be kept on the CoC's website.

Failure to comply with these policies and procedures may result in suspension or revocation of User access. Suspicion of unauthorized activity should be reported immediately to HMIS Lead Agency Staff.

Once the HMIS staff from the CoC Lead Agency have been contacted about an alleged violation, the HMIS staff will begin investigating the violation by collecting evidence and testimony from the parties involved. Higher importance will be placed on objective evidence of the infraction (such as audit reports) than subjective evidence (verbal or written testimony). After the evidence has been compiled, the violation will be considered by the appropriate level of oversight based on the level and frequency of violation (First and Second Violation: HMIS Staff, Third Violation: Per Governance Structure TBD). The User and CHO will be notified in writing once a decision has been determined. If the User is found to have violated the HMIS operational policies, the appropriate penalties will be levied as described above. The investigation will be treated as confidential; nobody outside of the HMIS staff and those involved in the investigative process will be made aware of the ongoing investigation. However, the outcome of the investigation will be available to HMIS staff upon request, but not shared publicly unless deemed necessary by the HMIS staff.

4. Organization and Management of BostonHMIS

I. Project Management

POLICY The Mayor's Office of Housing (MOH), City of Boston is responsible for project management and coordination of the BostonHMIS. The BostonHMIS Lead Staff is the primary contact for necessary or desired system-wide changes. In this role, the BostonHMIS Lead Staff endeavors to provide a uniform HMIS for the entire Boston CoC that yields the most consistent data for client management, agency reporting, and service planning.

Procedure All requests relating to the policies and procedures of the HMIS should be addressed with the BostonHMIS Lead Staff through the HMIS Helpdesk.

II. System Administration

POLICY The Mayor's Office of Housing (MOH) provides System Administration for both the Clarity HMIS application and the Data Warehouse and is responsible for baseline training, system changes, reporting, custom reporting, addressing end-user tickets and system coordination and administration. In the absence of the System Administrator, a member of the BostonHMIS Lead team may backup proxy responses to CHOs/Authorized Agencies and end users.

PROCEDURE The BostonHMIS System Administrators administer the day-to-day operations of the Clarity HMIS application and the Data Warehouse as governed by City of Boston CoC Bylaws, Code of Conduct and the BostonHMIS Policies and Procedures (this document). The Code of Conduct governs access to the Boston CoC's data (client level or otherwise). MOH is ultimately responsible for all final decisions regarding planning and implementation of the BostonHMIS.

III. HMIS Agency Management: Agency Manager

POLICY

Each Authorized Agency or Covered Homeless Organization (CHO) (regardless of front-end data system) must designate a staff member to be the HMIS Agency Manager who is responsible on a day-to-day basis for enforcing the data and security requirements under these Policies and Standard Operating Procedures. While one person per Authorized Agency may be designated as the Agency Manager, a backup Manager should be considered.

PROCEDURE

The Executive Director of the Authorized Agency must identify an appropriate Agency Manager, and provide that person's name, and contact information to the BostonHMIS System Administrators. Changes to that information over time should be reported immediately to the BostonHMIS System Administrators. The BostonHMIS Lead Staff is responsible for maintaining a current list of Agency Administrators.

Agency Administrators are responsible for the following:

- Serves as the primary contact between the Authorized Agency and the BostonHMIS System Administrator and the HMIS Lead.
- Ensures adherence to all Policies and Procedures contained in this manual.
- Must have a valid email address and be an active (logged in within the past 30 days), trained user.
- Communicates the need to remove end users from the BostonHMIS immediately upon termination from the agency, personal extended leave, placement on disciplinary probation, or upon any change in duties not necessitating access to BostonHMIS information. All changes must be relayed to the Boston CoC Help Desk.
- Has access to all client data, user data, and agency administration information for the Authorized Agency; thus, is responsible for the quality and accuracy of this data.
- Ensures the stability of the agency connected to the Internet and the BostonHMIS Clarity and Data Warehouse systems,

either directly or in communication with other technical professionals.

- Ensures Privacy Posting is posted and visible to all clients.
- Monitors and enforces compliance with standards of client confidentiality and ethical data collection, entry, and retrieval at the agency level.

IV. Communication with Authorized Agencies

POLICY The BostonHMIS Lead Staff is responsible for relevant and timely communication with HMIS Agency Managers. The BostonHMIS Lead Staff will communicate system-wide changes and other relevant information to agencies as needed.

PROCEDURE General communications from the BostonHMIS Lead Staff will be directed toward all users. Specific communications will be addressed to the person or people involved. The BostonHMIS Lead Staff will be available via the HMIS Helpdesk. The BostonHMIS email list will also be used to distribute HMIS information.

HMIS Agency Managers are responsible for distributing information to any additional people at their agency who may need to receive it, including, but not limited to, Executive Directors, client intake workers, and data entry staff.

V. Inter-Agency Data Sharing

Clarity

POLICY BostonHMIS Clarity is a “semi-open” system, meaning that basic client profile data is shared between all BostonHMIS participating agencies.

EXPLANATION The Clarity system is designed to achieve a one-to-many client to services record, improving data quality and deduplication while still safeguarding client confidentiality.

PROCEDURE When new clients are entered into Clarity, the initiating user must inform the client of the uses and disclosure of their personal data and the ability of the client to opt out of data sharing. If the client decides to Opt-Out of sharing, the Client Data Sharing Revocation of

Consent form must be completed and maintained in the client's file, and the Information Release in HMIS must be updated for all household members.

Users may be monitored to ensure compliance with this policy at any time by Agency Administrators, the CoC Monitoring entity, or the BostonHMIS System Administrators. If violations occur, the user may be subject to being permanently banned from BostonHMIS and may face possible legal action. If a user feels it is in the best interest of the client, they may request further restriction of the client's electronic sharing by submitting a ticket via the helpdesk.

Warehouse Sharing

The Boston HMIS Warehouse contains HMIS data from multiple front-end systems in the Boston CoC (Clarity, ETO). Client data and records are only available across agencies if the client has a Homeless Assistance Network (HAN) release on file in the Warehouse. If the client does not have a HAN release, the client record can only be seen by the age

.

VI. Ethical Data Use

POLICY

Data contained in the BostonHMIS will only be used to support or report on the delivery of homeless and housing services in the City of Boston. Each BostonHMIS End User will affirm the principles of ethical data use and client confidentiality contained in the BostonHMIS Policies and Procedures Manual, the Boston HMIS Agency Participation Agreement, and the Boston HMIS End User Agreement. Each Authorized Agency must have a written privacy policy, including specific policies related to employee misconduct or violation of client confidentiality. All Boston HMIS End Users are expected to understand their Agency's privacy policy.

PROCEDURE

All Boston HMIS users will sign a Boston HMIS System End User Agreement before being given access to the BostonHMIS Clarity live system. Any individual or Authorized Agency misusing, or attempting to misuse BostonHMIS data will be denied access to the database, and his/her relationship with the BostonHMIS may be terminated. Any Authorized Agency for which the relationship with the BostonHMIS is terminated may likely put funding in jeopardy by the Continuum of Care because of the statutory requirement to participate in the Continuum's HMIS.

5. System Management

I. System Availability

POLICY BostonHMIS will provide a highly available database server and will inform users in advance of any planned interruption in service.

EXPLANATION A highly available database affords agencies the opportunity to plan data entry, management, and reporting according to their own internal schedules. Availability is the key element in maintaining an HMIS that is a useful tool for Authorized Agencies to use in managing programs and services.

PROCEDURE No computer system achieves 100% uptime. Downtime may be experienced for routine maintenance, in the event of a disaster, or due to systems failures beyond the control of BostonHMIS System Administrators or the BostonHMIS Lead Staff. In the event of disaster or routine planned server downtime, the BostonHMIS Lead Staff will inform users of the cause and duration of the interruption in service.

Clarity Human Services

Bitfocus provides real-time information on the system status and incidence reports for Clarity Human Services, Reporting, Data Analytics, DIT API, Clarity Outreach, the Bitfocus website, and the Bitfocus Help Center.

The HMIS Clarity system is backed up every four hours and the entire system is backed up daily so it can be restored as quickly as possible if necessary. System Status updates for Clarity HMIS can be monitored by checking the System Status at http://status.bitfocus.com.

Boston HMIS Data Warehouse

Green River is available for real-time information on the system status and incidence reports for the Warehouse application, and its Reporting tools. BostonHMIS will provide a highly available database server and will inform users in advance of any planned interruption in service.

No computer system achieves 100% uptime. Downtime may be experienced for routine maintenance, in the event of a disaster, or due to systems failures beyond the control of BostonHMIS System Administrators or the BostonHMIS Lead Staff. In the event of disaster or routine planned server downtime, the BostonHMIS Lead Staff will inform users of the cause and duration of the interruption in service. The Boston HMIS Warehouse system is backed daily for 2 weeks so it can be restored as quickly as possible if necessary. System Status updates and incidence reports for the HMIS Warehouse are available from the software vendor but are not externally accessible. Boston's SLA with the software vendor requires the vendor to promptly notify Boston of any unplanned outages.

ETO Software Systems

EA and Agency Managed ETO Software Systems must have processes and documentation in place to communicate the Systems Availability or planned interruption of service to all users.

Comparable Databases

Agency Managed Comparable Databases must have processes and documentation in place to communicate the Systems Availability or planned interruption of service to all users.

II. Data System Monitoring and Performance Evaluation

POLICY The BostonHMIS Lead Staff will regularly monitor and evaluate the effectiveness of the BostonHMIS Implementation and, based on the information received, will continue to make enhancements to the BostonHMIS system and the Policies and Standard Operating Procedures as necessary.

EXPLANATION Monitoring and evaluation help ensure the security and proper usage of the BostonHMIS system.

PROCEDURE The BostonHMIS System Administrators will conduct internal system monitoring. This information will be shared with the CoC and may be used by the CoC to monitor programs funded through the CoC as required by HUD.

III. Project Set-up

Clarity

POLICY BostonHMIS System Administrators will create new projects in Boston's Clarity unless special permission is given to a CHO's Agency Administrator. All new projects will be configured with HUD Project Descriptor Data Elements (PDDE), and Program Specific Data Elements (PSDE) as defined in the HMIS Data Standards.

PROCEDURE A CHO's will complete and submit a New Project Request Form to BostonHMIS Admins to create the new project in Clarity.

If special permission has been granted to an Agency Administrator, the new project is to be created in the Clarity Training site, then submit a HelpDesk Case for final review and approval by BostonHMIS Administrators prior to the creation of the project in the live site.

Vendor resources related to this policy are included in the Clarity Human Services Help Center[2]

To keep project names consistent across HMIS, grant management applications, and federal reporting, the project name will be the same grant name.

Boston HMIS Data Warehouse

The Boston HMIS Data Warehouse is read-only when it comes to HMIS data from front-end systems like Clarity and ETO. No project setup is done within the Boston HMIS Data Warehouse.

ETO Software Systems

EA and Agency Managed ETO Software Systems should have a process in place to ensure that projects will be configured with HUD

[2] https://help.bitfocus.com/how-to-set-up-a-program-detailed-instructions

Project Descriptor Data Elements (PDDE), and Program Specific Data Elements (PSDE) as defined in the HMIS Data Standards.

To keep project names consistent across HMIS, grant management applications, and federal reporting, the project name will be the same grant name.

Comparable Databases

Agency Managed Comparable databases should have a process in place to ensure that projects will be configured with HUD Project Descriptor Data Elements (PDDE), and Program Specific Data Elements (PSDE) as defined in the HMIS Data Standards.

To keep project names consistent across HMIS, grant management applications, and federal reporting, the project name will be the same grant name.

IV. Minimal Technical Standards

Clarity and BostonHMIS Data Warehouse

POLICY

Each Agency is responsible for providing and maintaining computer hardware and Internet service as appropriate to their HMIS front-end application, helpdesk and training tools. Clarity HMIS requires an up-to-date web browser to access all the software's features.

PROCEDURE

Agencies will annually review and update to current industry standards their intranet and internet software and security measures. All other data security measures in Section 7 (Data Security Requirements), including user authentication, must be adhered to.

Intranet Specifications and Requirements

Agencies utilizing an Intranet must work with their IT departments to ensure HMIS, helpdesk, and training tools are accessible by end users in the organization.

Workstation Specifications and Requirements

Clarity Human Services requires an up-to-date web browser to access all of the software's features. To ensure the latest security features are in place, we strongly recommend always using the latest version of a supported web browser. Bitfocus supports the most recent version of the following web browser for accessing Clarity Human Services:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Apple Safari

You can access information regarding the current browser you are using here: https://www.whatsmybrowser.org

All computers that access HMIS should have up to date antivirus software, and be password protected.

Internet Connectivity Specifications

Connecting to the internet via an unsecured network may expose client data. Here are a few resources published by major internet providers on securing your wireless network:

- Cox - Ways to Secure Your Wireless Network
- Xfinity - Differences in Your Xfinity WiFi Network - Secure vs. Open Connections
- AT&T - Enable your Wi-Fi network security - Pace 5031

ETO Software Systems

EA and Agency Managed ETO Software Systems have access to a Browser FAQ as certain features must be accessed via compatibility mode.

Comparable Databases

Agency Managed Comparable Databases must ensure that devices are compatible with their software requirements.

VI. System Access and User Authentication

Clarity

POLICY

Only the BostonHMIS System Administrators are authorized to grant user access to the BostonHMIS-supported front-end system (Clarity). User accounts will be unique for each user and may not be exchanged or shared with other users

EXPLANATION

Unique usernames and passwords are the most basic building block of data security. Not only is each user name assigned a specific access level, but in order to provide clients or program management an accurate record of who has altered a client record, when it was altered, and what the changes were (called an "audit trail") it is necessary to log a user name with every change. Exchanging or sharing usernames seriously compromises the security of the BostonHMIS system, and will be considered a breach of the system user agreement and will trigger appropriate repercussions and/or sanctions for the user and agency.

PROCEDURE

Users are not able to access any data until they have completed the Boston CoC training modules for their access level, all HMIS Participating Agency and HMIS End User agreements are executed, and the account is activated by BostonHMIS staff. The BostonHMIS Lead agency staff will have access to the list of active end user names.

The HMIS Participating Agency shall designate one User to be the Agency HMIS Manager/ Site Manager, who will identify and approve the agency's respective users, and determine Clarity software user access level for their respective users. The level will be based on each user's job function as it relates to the Clarity software's data entry and retrieval schema. The System Administrators shall aid in the determination of HMIS User access level when requested. Additionally, Agency HMIS Manager/ Site Manager will monitor the users in their agency to ensure that accounts are current.

Eligible Users

- To be eligible as a user of the BostonHMIS, the user must:

- Work for an agency that has signed a Partner Agency Agreement, works for the HMIS Lead Agency, or is under a legally binding contract with the HMIS Lead Agency. This includes volunteers and any person in a non-employee, consulting, or contractual status with either the service providers or the HMIS Lead (for example, consultants and researchers).
- Have signed the BostonHMIS User Agreement Form
- Completed all required training related to HMIS and Clarity

Boston HMIS Data Warehouse

Users are not able to access the Warehouse until they have completed the Boston CoC training modules for their access level, all HMIS Participating Agency and HMIS End User agreements are executed, and the account is activated by BostonHMIS staff. The BostonHMIS Lead agency staff will have access to the list of active end-user names.

The HMIS Participating Agency shall designate one User to be the Agency HMIS Manager/ Site Manager, who will identify and approve the agency's respective users, and determine Warehouse software user access level for their respective users. The level will be based on each user's job function as it relates to the data and reporting accessible in the Warehouse. The System Administrators shall aid in the determination of HMIS User access level when requested. Additionally, Agency HMIS Manager/ Site Manager will monitor the users in their agency to ensure that accounts are current.

ETO Software Systems

EA and Agency Managed ETO Software System administrators are encouraged to set similar best practices for End User Access and Authorization and be documented in the Agency's manual.

Comparable Databases

Agency Managed Comparable Databases administrators are encouraged to set similar best practices for End User Access and Authorization and be documented in the Agency's manual.

IX. User Access Levels

POLICY All BostonHMIS Users will have a level of access to data that is appropriate to the duties of their position so that information is recorded and accessed on a "need to know" basis. All users should have the level of access that allows efficient job performance without compromising the security of the BostonHMIS or the integrity of client information.

PROCEDURE Each HMIS Agency Manager, or proxy, will identify the level of access each end user will have to the BostonHMIS database and front-end software systems. Privilege levels are detailed in Appendix - User Access Role Matrix.

X. New User Access

Clarity

POLICY This policy applies to any organization requesting access to the Clarity Live and Training Sites.

All first-time users must complete all training required by BostonHMIS before access to the Clarity Live Site. This is to ensure that end users have basic knowledge of the system and important HMIS topics, such as data quality, client privacy, and data security.

Requests for access to the Clarity Live and Training Sites must be made by Agency HMIS Managers, or a person of authority designated by an agency to authorize requests. This is to ensure that Agency HMIS Managers know who is being given access to the Clarity Live Site on their behalf. A person may not request access to the Clarity Live and Training Sites for themself outside of authorized submitters.

All requests for access must be made through the BostonHMIS Helpdesk and all correspondence related to the request will be handled through the Salesforce ticket management software.

EXPLANATION Reason for Policy:

- To provide a consistent method for requesting User Access to the BostonHMIS/BostonClarity Live Site

- To support the HMIS Lead agency’s responsibility to protect the integrity of the BostonHMIS/BostonClarity Live Site by documenting:
    - Who has access to the Boston Data Warehouse
    - Who has access to the BostonClarity Live and Training sites.
    - Reason for needing access.
    - Who authorized the access.
- To ensure that all users accessing the Clarity Live Site have completed basic training on data entry, data quality, client privacy, and data security.

PROCEDURE

Agency HMIS Managers/Site Managers must submit a *Request for Access* for users to the BostonHMIS HelpDesk. All communication related to the request will be managed through the HelpDesk.

Requesting access to the Clarity Live Site is a three-step process:

1. A new user request must be submitted to the BostonHMIS Helpdesk for pre-access training.
2. The new user must complete the assigned training courses.
3. Once training is completed, a second request for new user access must be submitted to the BostonHMIS Helpdesk.

<u>Step 1. Request New User Pre-Access Training</u>

- A new user pre-access training request must be submitted to the BostonHMIS Helpdesk. The request must include
    - Requestor's Name and Contact Information
    - Organization Name
    - New End User’s Name and Contact Information
        - Email
        - Phone/Cellphone (including extensions)
    - New End User Manager Name/Contact Information

- The Type of Access Requested as the Request Title. Access Options include:
    - New User - Live Site
    - New User - Training Site

    - New User - Learning Management System (LMS)

- The Level of Access Level Needed. Access Level Options include:
    - Agency Staff
    - Referral Staff
    - Agency Site Manager
    - Agency Manager
    - System Administrator
- Any special training the agency would like the user to receive.
- The new user will be provided credentials to access the Boston CoC Learning Management System (LMS) and enrolled in required courses.
- The new user will also be provided credentials to the Clarity Training Site for the purpose of practicing data entry.
- The new user, the requester, and the new user's manager (if applicable) will receive an email via the BostonHMIS Helpdesk (Salesforce) that provides credential information for the LMS and the Clarity Training Site, URLs to the LMS and Clarity Training Site, instructions on how to proceed with completing training, and links to additional resources related to data entry in Clarity.
- The requester will receive a second email via the BostonHMIS Helpdesk (Salesforce) informing them the case is closed and reminding them to monitor the new user's training progress via system-generated reports.

<u>Step 2. The New User Completes the Required Training</u>

BostonHMIS will enroll new users in required training prior to the credentials notification email in Step 1.

- The Boston CoC LMS will send an email for each course enrollment, which will include the course link.
- The Boston CoC LMS will notify the BostonHMIS Team when courses are completed.
- The BostonHMIS Team will update the Clarity New User Access Tracker with course completion dates.

- When the user completes all the required courses, the user will be marked as approved for access to the Clarity Live Site in the Clarity New User Access Tracker.
- Agency HMIS Managers may request new user access to the Clarity Live Site as soon as the new user is marked as approved for access.

Step 3. The Agency HMIS Manager Requests New User Access to the Clarity Live Site

- A new user Clarity Live Site access request must be submitted to the BostonHMIS Helpdesk. The request must include
    - Requestor's Name and Contact Information
    - Organization Name
    - New End User’s Name and Contact Information (Email, phone/cellphone including extensions)
    - New End User’s Manager Name/Contact Information
- The Type of Access Requested as the Request Title. Access Options include:
    - New User - Live Site
    - New User - Training Site
    - New User - LMS
- The Level of Access Level Needed in the Clarity Live Site. Access Level Options include:
    - Agency Staff
    - Referral Staff
    - Agency Site Manager
    - Agency Manager
- Any additional agencies to which the new user should be given access.
- The new user will also be provided credentials to the Clarity Live Site.
- The new user, the requester, and the new user’s manager (if applicable) will receive an email via the BostonHMIS Helpdesk (Salesforce) that provides credential information for the Clarity Live Site, the URL to the Clarity Live Site, and notification that the request has been closed.

A visual representation of this workflow is available here.

Boston HMIS Data Warehouse

Agency HMIS Managers/Site Managers must submit a *Request for Access* for users to the BostonHMIS HelpDesk. All communication related to the request will be managed through the HelpDesk. Agency HMIS managers must submit a Warehouse authorization form for the users they are requesting access. The form must include the user's name, e-mail address, and level of access that is being requested. This form must be signed by the Agency HMIS manager. A copy of this form can be found in the appendix of this document.

Once a ticket is submitted and an authorization form is received, the Warehouse accounts will be created. Users will receive an email informing them of their Warehouse account, and a link will be provided to activate the account. This link will be valid for 2 weeks from when the account was created.

Upon first logging in, users will be directed to an LMS training module for the Warehouse. The user will not be able to access the Warehouse until this training module is completed. Once complete, the user will have access to the Boston HMIS Warehouse.

ETO Software Systems

EA and Agency Managed ETO Software Systems should replicate a similar training process for users before access is granted to the system. It is the responsibility of the administrators of the Software to ensure that all users are trained appropriately in the system. The Boston CoC LMS has some basic ETO training available if the Organization would like to utilize these resources.

Comparable Databases

Agency Managed Comparable Databases should replicate a similar training process for users before access is granted to the system. It is the responsibility of the administrators of the Software to ensure that all users are trained appropriately in the system. The Boston CoC LMS has basic training available regarding the data elements that are required to be collected however there is no staff with relevant experience in many of the comparable databases in use to create specific training. It is incumbent upon the Administrator of the system to ensure that end users receive the proper training on the system in use.

Coordinated Entry Agency - Housing Needs Assessment User Access (Clarity Only)

POLICY All end users accessing the Coordinated Entry agency – Housing Needs Assessment project must complete training as required by the CE Operator and BostonHMIS before being approved for access. This training may be in addition to training requirements for new Clarity users and Clarity account reactivations but also applies to existing users whose job responsibilities now require access to the Housing Needs Assessment program.

EXPLANATION Accurate information about client's service use is the foundation upon which clients are prioritized for housing in Boston. It is imperative that end users optimize a client's chance of accurate matching by providing highly accurate information. Requiring training on how the collection, enter, and use high quality data is a key component to ensuring data accuracy. This policy also ensures a consistent method for requesting User Access to the Coordinated Entry agency – Housing Needs Assessment project and supports the HMIS Lead agency's responsibility to protect the integrity of the BostonHMIS/BostonClarity Live Site by documenting:

Who has access to the Coordinated Entry Agency and the Housing Needs Assessment project, Reason for needing access, Who authorized access.

PROCEDURE:

The following procedures must be followed to request access to the Coordinated Entry agency – Housing Needs Assessment project in Clarity Live:

1. Agency HMIS Managers/Site Managers or a person of authority designated by an agency to authorize requests must submit to the Coordinated Entry Operator a Request for Access to the Coordinated

Entry agency - Housing Needs Assessment for the user. A person may not request access to the Coordinated Entry agency - Housing Needs Assessment for themself outside of the authorized submitters. All communication related to the request will be managed through the CE Team email (Ceteam@homestart.org). The request must include:

a. The user's name and email

b. Purpose for needing access to the Coordinated Entry agency - Housing Needs Assessment project

c. Current Access Status (New Clarity User or Existing Clarity User)

d. Additional persons who should be notified of the access approval process

2. The CE Operator team will submit all requests for access through the BostonHMIS Helpdesk and all correspondence related to the request will be handled through the Helpdesk ticket management software. The CE Operator can request the following types of access:

- New User: Clarity + Pathways
- New User: Clarity + RRH2PSH
- New User: Clarity + Pathways + RRH2PSH
- Existing User: Pathways
- Existing User: RRH2PSH
- Existing User: Pathways + RRH2PSH
- Account Reactivation that also requires retraining on assessments

3. If the proposed user will be a new Clarity user or reactivated user, the procedure for user access is the same as the Clarity New User/User Reactivation Access policy but requires additional training for coordinated entry purposes. The end user must complete all required training before being given access to the Coordinated Entry agency - Housing Needs Assessment.

XI. End User Account Reactivation

Clarity

POLICY

All End User accounts for both the training and live sites for the Clarity software will automatically deactivate after 60 days of inactivity. To reactivate an end-user account, Agency Administrators/Site Managers must submit a *Request for Access* for users to the BostonHMIS HelpDesk for access to the applicable site. This is to ensure that Agency Administrators/Site Managers know who is being given access to the live site on their behalf.

All end users requesting reactivation of Clarity Live Site credentials, whose account has been inactive for 90 days or more, must complete all training required by BostonHMIS before access to the Clarity Live Site is reactivated.

In addition, the Clarity software requires users to log in to the site the same day their account is reactivated by a System Administrator. If the user does not log in on the same day, Clarity will automatically deactivate the account the next day at 5:30 am.

End Users will receive an email notification one week before their accounts are set to expire. To avoid deactivation, the user simply needs to log in.

PROCEDURE

To request a reactivation of an account, Agency Administrators/Site Managers must submit a *Request for Access* for users to the BostonHMIS HelpDesk for access to the applicable site. The Request for Access must include all components required for *Requesting New User Access* and include the following additional information:

- The End User's work schedule.
- The email addresses for any other supervisor or staff that should be copied on the resolution email.

A BostonHMIS System Administrator will review the case for the required information and will do one or more of the following:

- Contact the Agency Manager if the user's email address and/or schedule is missing,

- Contact the Agency Manager and End User informing them of day of when the account will be reactivated (if not the same day), or
- Reactivate the End User's account the same day (if the End User is available) and email both the Agency Manager and End User once the account has been reactivated and is ready for login.

End Users must log in as soon as possible or by the end of the day and respond back to System Administrator's email confirming whether or not they successfully logged in to Clarity.

If the End User does not log in as required to reactivate the account, the Agency Manager will notify the End User's immediate manager of their failure to do so.

Agency Administrators must follow up with End Users to confirm they received the email and were able to log in to the site. Agency Manager must then notify BostonHMIS of the confirmation so that the case can be closed.

If the End User is unable to log in after the account has been reactivated, the End User or Agency Manager will respond back to the case informing the System Administrator of the issue. The System Administrator will troubleshoot the issue until resolved. Communication will continue via the case until the End User is able to login successfully.

Boston HMIS Data Warehouse

Boston HMIS Warehouse accounts that are inactive for 180 days will be automatically deactivated. In order to reactivate an account, the HMIS Agency Manager must submit a ticket to the Boston CoC Helpdesk. The ticket must include the user's name and e-mail address. Upon receipt, an HMIS team member will reactivate the user's account. Users will receive an email with a link to log in and reset their password.

ETO Software Systems

EA and Agency Managed ETO Software Systems should have similar processes and procedures in place to re-activate inactive user accounts. There should also be procedures in place for re-training as needed when inactive in a system after a set standard of time.

Comparable Databases

Agency Managed Comparable Databases should have similar processes and procedures in place to re-activate inactive user accounts. There should also be procedures in place for re-training as needed when inactive in a system after a set standard of time.

XII. Requesting Change in Access Level

Clarity Only

POLICY

Requests for changes in access level in the Clarity Live Site, the Clarity Training Site, and the Boston CoC Learning Management System (LMS) must be made by Agency HMIS Managers, or a person of authority designated by an agency to authorize requests. This is to ensure that Agency HMIS Managers know who has different access levels access to the Clarity Live Site on their behalf. A person may not request an access level change to the Clarity Live and Training Sites for themself.

A Change in Access Level Request may be made to increase a user's access level or to decrease a user's access level. A request for an increase in user access level may require the user to complete training before their access level increase is approved.

All requests for change in access level must be made through the BostonHMIS Helpdesk and all correspondence related to the request will be handled through the Salesforce ticket management software.

PROCEDURE

Agency Administrators/Site Managers must submit a *Request for a Change of Access Level* for users to the BostonHMIS HelpDesk. All communication related to the request will be managed through the HelpDesk.

Change In Access Level Request (No Additional Training)

Requesting a Change in Access Level that does not require additional training, such as a decrease in access level, is a one-step process:

- A *Change in Access Level Request* must be submitted to the BostonHMIS Helpdesk. The request must include
    - Requestor's Name and Contact Information
    - Organization Name
    - End User's Name and Contact Information
        - Email
        - Phone/Cellphone (including extensions)
    - New End User Manager Name/Contact Information
- The systems to which the Access Change Request applies. Options include:
    - Clarity - Live Site
    - Clarity - Training Site
    - Learning Management System (LMS)
- The Level of Access Level Needed. Access Level Options include:
    - Agency Staff
    - Referral Staff
    - Agency Site Manager
    - Agency Manager
    - System Administrator
- The requested effective date of the access level change.
- The reason for the access level change.

The BostonHMIS Team will review the Request, make the change, and provide verification of the Change in Access Level to the requestor, the user, and the user's manager (as applicable) via the BostonHMIS Helpdesk (Salesforce).

Requesting an Increase in Access Level

Requesting an increase in access level in the Clarity Live Site is a three-step process:

1. A *Change in Access Level - Training Request* must be submitted to the BostonHMIS Helpdesk for pre-access training, if needed.
2. The user must complete the assigned training courses if needed.

3. Once training is completed, a second request for a *Change in Access Level - Training Completed* must be submitted to the BostonHMIS Helpdesk.

<u>Step 1. Request Change in Access Level Pre-Access User Training</u>

A user pre-access change training request must be submitted to the BostonHMIS Helpdesk.

The request must include:

- Requestor Name and Contact Information
- Organization Name
- End User Name and Contact Information
    - Email
    - Phone/Cellphone (including extensions)
- End User Manager Name/Contact Information
- The systems to which the Access Change Request applies. Options include:
    - Clarity - Live Site
    - Clarity - Training Site
    - Learning Management System (LMS)
- The Level of Access Level Needed. Access Level Options include:
    - Agency Staff
    - Referral Staff
    - Agency Site Manager
    - Agency Manager
    - System Administrator
- The requested effective date of the access level change.
- The reason for the access level change.
- Any special training the agency would like the user to receive.

The end user will be provided/reactivated credentials to access the Boston CoC Learning Management System (LMS) and enrolled in required courses.

The end user will also be provided credentials to the Clarity Training Site for the purpose of practicing new access-level tasks.

The end user, the requester, and the end user's manager (if applicable) will receive an email via the BostonHMIS Helpdesk

(Salesforce) that provides credential information for the LMS and the Clarity Training Site, URLs to the LMS and Clarity Training Site, instructions on how to proceed with completing training, and links to additional resources related to the increased access level in Clarity.

The requester will receive a second email via the BostonHMIS Helpdesk (Salesforce) informing them the case is closed and reminding them to monitor the new user’s training progress in the System generated report.

Step 2. The End User Completes the Required Training

BostonHMIS will enroll the end user in required training prior to the credentials notification email in Step #1.

- The Boston CoC LMS will send an email for each course enrollment, which will include the course link.
- The Boston CoC LMS will notify the BostonHMIS Team when courses are completed.
- The BostonHMIS Team will update the Help Desk Case with course completion dates.
- When the user completes all the required courses, the user will be marked as approved for increased access in the Clarity New User Access Tracker.
- Agency HMIS Managers need to track end-user progress in the Clarity User Access Tracker and may submit the second request for Change in Access Level as soon as the new user is marked as approved for access level change.

Step 3. The Agency HMIS Manager Requests *Change in Access Level – Training Completed*

The request must include:

- Requestor Name and Contact Information
- Organization Name
- End User Name and Contact Information
    - Email
    - Phone/Cellphone (including extensions)

- The systems to which the Access Change Request applies. Options include:
    - Clarity - Live Site
    - Clarity - Training Site
    - Learning Management System (LMS)
- The Level of Access Level Needed. Access Level Options include:
    - Agency Staff
    - Referral Staff
    - Agency Site Manager
    - Agency Manager
    - System Administrator
- The requested effective date of the access level change.
- The reason for the access level change.
- Any special training the agency would like the user to receive.

The end user will be provided/reactivated credentials to access the Boston CoC Learning Management System (LMS) and enrolled in required courses.

The end user will also be provided credentials to the Clarity Training Site for the purpose of practicing new access-level tasks.

The end user, the requester, and the end user's manager (if applicable) will receive an email via the BostonHMIS Helpdesk (Salesforce) that provides credential information for the LMS and the Clarity Training Site, URLs to the LMS and Clarity Training Site, instructions on how to proceed with completing training, and links to additional resources placed to the increased access level in Clarity.

Boston HMIS Data Warehouse

Requests for a change in access level or permissions for the Boston HMIS Data Warehouse must be submitted by the HMIS agency manager through the Boston CoC Helpdesk. The request must include the user's name, e-mail address, the requested change in access level or permissions, and the reason for the requested change.

Once received, the Boston HMIS Data Warehouse support team will review the request, and pending any follow-up questions will make the requested changes to the user's account.

If there is LMS training associated with any of the requested permission changes, the training modules will be assigned to the user prior to granting the changes in permission.

ETO Software Systems

EA and Agency Managed ETO Software Systems should have similar processes and procedures in place to change the role of a user account. There should also be procedures in place for new training as needed when assuming new levels of access in the system.

Comparable Databases

Agency Managed Comparable Databases should have similar processes and procedures in place to change the role of a user account. There should also be procedures in place for new training as needed when assuming new levels of access in the system.

XIII. Termination of User Access

POLICY

Agency Administrators/Site Managers must notify BostonHMIS of the need to discontinue access to the training site through the HelpDesk within 24 hours that the need becomes known to the Agency Manager/Site Manager.

PROCEDURE

A request for Access Termination must include the following information:

- Requestor Name and Contact Information
- Organization Name
- End User Name and Contact Information
    - Email
    - Phone/Cellphone (including extensions)
- End User Manager Name/Contact Information
- Request Title: Request for Access Termination
- Indicate which sites need access termination
    - Live Site

    - Training Site
    - Warehouse
- Reason for Request
- Access End Date

XIV. Access to Core Database

POLICY

Only the BostonHMIS System Administrators/BostonHMIS Lead Staff or contracted designees will have direct access to the Boston HMIS database through any means other than the BostonHMIS user interface unless explicitly given permission by BostonHMIS System Administrators/BostonHMIS Lead Staff.

PROCEDURE

Boston HMIS Lead Staff will employ security methods to prevent unauthorized database access

XV. System Customization/ Configuration

Clarity Only

POLICY

Customizations to HMIS are separated into two categories: System-Wide and Agency-Specific. System-Wide customizations/ configurations affect all end users and the operations of HMIS. These changes may only be made by system administrators via system configurations and account settings. Requests to review these settings must be requested through helpdesk. System-Wide changes must also be logged by the BostonHMIS in a release note or change log and made public to Agency Administrators. System-Wide changes are also expected as part of vendor software upgrades with data standards, etc. Vendor release notes may be made available by request.

Agency-Specific customizations are accessible by the Agency Manager role in the application. These changes must be mocked up in the training environment and tested prior to creation on the live site. Customizations beyond the scope of the agency manager role in the application must be requested through the helpdesk and approved via a to-be-determined process and procedure.

PROCEDURE Boston HMIS System Configuration Process DRAFT, BostonHMIS Policy Committee Voting Process DRAFT

XVI. Boston HMIS Clarity Training Site Management

Clarity Only

POLICY To facilitate creativity and innovation in the use of the Clarity HMIS software, provide a safe environment for new staff to learn data entry protocols, and test new functionality, custom scenarios, and reporting, BostonHMIS will provide, upon request, access for BostonHMIS Participating Agency staff to a Clarity software training environment ("training site") that, to the extent possible, mimics the live Clarity database.

PROCEDURE The training site may be used to:

- Create and test custom screens, fields, and workflows
- Create and/or test custom functionality and advance uses of the Clarity software
- Create new user training scenarios, including agencies, programs, services, and clients
- Train new agency staff on data entry protocols
- Custom reporting development for System Admin approval

The training site may be used to meet the training requirements for System Administrators.

Agency Administrators/Site Managers retain responsibility for the integrity of the training site and the actions of their authorized staff.

Restrictions:

1. Sharing of usernames and passwords is not allowed and all data system integrity and security policies must be followed, including termination of user rights in the event of staff turnovers.

2. Training site users are not authorized to edit custom fields, screens, and templates that they did not create without written permission from the agency of ownership.
3. Training site users are not authorized to edit another agency's information, fields, screens, and set-ups without written permission from the agency of ownership.
4. It is not allowable for Clarity training site users to enter the name and personal information of a known person experiencing or at-risk of experiencing homelessness. The situation of a person under these circumstances may be mimicked in the training site using fictional elements of personal protected information.

Limited Liabilities:

1. BostonHMIS is not responsible for activities conducted by users authorized by Agency Manager/Site Managers, including fixing program deletions, improperly set up programs and services, or use of real person data in the training site environment.
2. BostonHMIS is not responsible for providing help desk support for customization created on the training site, including custom training that is not developed by the BostonHMIS team.

Failure to adhere to these policies will result in suspension of access to the training site until mediation has occurred. Mediation may include reparations for damage done to the system, another agency, and cost related to rebuilding the training site.

User Access

The policies and procedures for access, account reactivation, and termination of access to the training site is the same as the User Access protocols for the live Clarity site.

The end user's username is always the first initial of their first name and their last name (ex. Katie Bell would be kbell).

If a user has forgotten their password for the training site, they must submit a request for a password reset to the HMIS HelpDesk in accordance with the policies and procedures associated with the live Clarity site.

XVII. Technical Support and Help Desk

Training Requirements

- Participants are responsible for any basic computer training required of its users.
- All Users are required to attend HMIS Software training sessions as directed. Online training and refreshers are available.
- The System Administrators will be responsible for:
    - Training new Participating Agencies
    - Training of all Agency Administrators in the use of Clarity Software within reasonable constraints
    - Directing or training End-Users in the use of Clarity Software within reasonable constraints

Helpdesk Requirements

Helpdesk tickets will be reviewed M-F between 8 am – 5 pm. Tickets will have an initial response within 24 hours; the final resolution will be dependent on the ticket type and complexity of the request. Updates to open tickets will be reviewed and made within a 7 window. Tickets will be escalated to the vendor as needed. Development and report requests may be subject to further vetting.

Tickets that have had no activity in 45 days will be closed automatically.

The Help Desk can be found at:

https://www.boston.gov/departments/housing/boston-continuum-care-coc-help-desk

6. Data Collection Requirements

I. Minimum Data Collection Standard

POLICY All programs contributing data to HMIS must adhere to the most current data collection requirements of the HUD HMIS requirements outlined by the HMIS Data Standards and the HMIS Data Manuals including the Universal Data Elements(UDEs). The UDEs are the basis for producing unduplicated estimates of the number of people experiencing homelessness accessing services from homeless assistance projects, basic demographic characteristics of people experiencing homelessness, and patterns of service use, including information on shelter stays and homelessness over time. See the list of Universal Data Elements and Boston's City of Origin question, and Program Specific Data Elements in the Appendices.

PROCEDURE Federally funded programs must follow the data requirements set forth in the HMIS Manual for that funding source. The UDEs, and Boston's City of Origin questions are required to be collected by all projects participating in an HMIS, regardless of funding source.

Transmitting Agency Data Contribution Requirements

POLICY Agencies providing data to BostonHMIS must adhere to all data collection requirements and will upload data in the authorized .CSV format on a schedule agreed upon by the agency and MoH.

PROCEDURE To accommodate the regular transmission of data from front-end systems to BostonHMIS, participating agencies must adhere to the following procedures.

- Each Agency is responsible for providing and maintaining computer hardware and Internet service in conjunction with use of an HMIS.
- The Transmitting Agency shall designate one User to be the Site Manager and be responsible for the transmittal of data via the hmis.boston.gov secure web portal for inclusion in the Boston HMIS Data Warehouse.
- The Transmitting Agency may have the option when available to automate this transmission of data in conjunction with their front-end software provider and the Boston HMIS Data Warehouse vendor.

II. Project Sponsor Data Responsibilities

POLICY The City of Boston encourages service delivery partnerships between agencies and recognizes the opportunity for collaboration through shared programs and subcontracts with small service providers. However, the primary sub-recipient of all City and CoC funds will maintain responsibility for the collection and quality of data collected and contributed to the HMIS, either directly or indirectly. This is to ensure that sub-sub-recipients are monitored for data quality and sub-recipients have access to program data for required reporting.

Applicability: All Service Providers

Data Responsibility Policy: Project Sponsors are responsible for ensuring the collection and input of required HMIS data in the HMIS. This responsibility extends to the collection and input of data acquired by any sub-recipients and contractors utilized by the project sponsor to fulfill the obligations of the grant award/contract. This responsibility must be included in all contracts and contracts must include specific conditions and procedures for acquiring, inputting, and retention of client records obtained through the program's activities.

PROCEDURE

Project Sponsors must provide forms and tools to the project sponsor and sub-recipient/contractor staff that assures the correct collection and input of required project data in accordance with established data quality, data privacy, and data security policies and procedures. In the event that the project sponsor chooses to utilize a sub-recipient or contractor to fulfill its program obligations, additional required procedures are

Contract Requirements: All contracts for services, project sponsor, sub-recipient, or otherwise, to be rendered paid for by federal monies must include the following required components:

1. All End Users, including sub-recipients and contractors of the project sponsor must be covered by data security liability insurance and must provide proof of adequate coverage to MoH as a condition of the grant award.
2. All persons collecting or otherwise having access to the personal protected information of homeless clients must sign an end-user agreement that binds them to HMIS policies and procedures, including data quality, privacy, and security requirements, regardless of whether a project sponsor or

sub-recipient/contractor, and that set forth disciplinary actions for proven breaches of proper data handling.

3. All forms of data collection, paper or otherwise, other than direct input into the HMIS, if the data is collected by the subrecipient or contractor for the purposes of fulfilling the project sponsor's program's data collection requirements cannot be retained, by copy, scan, photograph, or other retention methods.

III. Data Quality Plan

POLICY

The HUD HMIS Data Standards define specific data elements that must be collected and entered into HMIS. HUD defines two categories of data elements: Universal Data Elements - required to be collected from all homeless clients served by any CHO, and Program Specific data elements - collected from all clients if the CHO receives HUD grant funds (i.e. Continuum of Care, Emergency Solutions Grant, SSVF, RHY, PATH, and HOPWA).

PROCEDURE

See Appendices for the most recent Boston HMIS Data Quality Improvement Plan. Not adhering to the guidelines specified in the HMIS Data Quality Plan can impact a CHOs performance monitoring evaluation. CoC's reserve the right to levy penalties or fines for not adhering to Data Quality standards.

IV. Warehouse Requirements

Transmitting Agency Data Contribution Requirements

POLICY

Agencies providing data to BostonHMIS must adhere to all data collection requirements and will upload data in the authorized .CSV format on a schedule agreed upon by the agency and MoH.

PROCEDURE

To accommodate the regular transmission of data from front-end systems to BostonHMIS, participating agencies must adhere to the following procedures.

- Each Agency is responsible for providing and maintaining computer hardware and Internet service in conjunction with the use of an HMIS.

- The Transmitting Agency shall designate one User to be the Site Manager and be responsible for the transmittal of data via the hmis.boston.gov secure web portal for inclusion in the Boston HMIS Data Warehouse.
- The Transmitting Agency may have the option when available to automate this transmission of data in conjunction with their front-end software provider and the Boston HMIS Data Warehouse vendor.
- If choosing not to automate this process, the Site Manager for the agency will be responsible for regularly uploading their agency's HMIS data in the authorized CSV format to the Boston HMIS Data Warehouse at least monthly.

V. HMIS Data Protection

POLICY All BostonHMIS end users will have a level of access to data that is appropriate to the duties of their position so that information is recorded and accessed on a "need-to-know" basis. All users should have the level of access that allows efficient job performance without compromising the security of the BostonHMIS or the integrity of client information.

PROCEDURE Each Agency HMIS Manager/Site Manager will identify the level of access each end user will have to the BostonHMIS and will request access to the system in accordance with Section 4 of these policies and procedures, Requesting New User Access or Requesting User Access Change.

BostonHMIS end users will maintain the security of any client data extracted from the database and stored locally, including all data used in custom reporting. BostonHMIS end users will not electronically transmit any unencrypted client data across a public network. Any custom reports (electronic or printed) which are shared with a non-Participating agency, must remove Client and Household names. Agencies engaging research consultants or contractors, including research associated with state or federally-funded research efforts, must execute legally binding agreements with said consultants or contractors that include specific language binding them to compliance with all BostonHMIS policies and procedures.

The City of Boston maintains a Code of Ethics that strongly supports the ethical use of data to support or report on the delivery of homeless and housing services, including ensuring client privacy and confidentiality from unauthorized persons. This extends to the protection of data and information generated from the HMIS in whatever form it is extracted and ultimately made viewable (MS Excel, MS Word, data dashboards, reports, public documents, research documents, etc.).

Data extracted from the database and stored locally will be stored in a secure location (not on DVDs/CDs or other temporary storage mechanisms like flash drives or on unprotected laptop computers, for example) and will not be transmitted outside of the private local area network unless it is properly protected via encryption or by adding a file-level Password. The BostonHMIS System Administrators will provide help in determining the appropriate handling of electronic files. All security questions will be addressed to the BostonHMIS System Administrators via the HMIS Helpdesk. Breach of this security policy will be considered a violation of the user agreement, which may result in personnel action and/or agency sanctions.

7. Privacy and Confidentiality Requirements

I. Baseline Privacy Policy

POLICY

The BostonHMIS System operates under implied consent to collect, accept, manage, and share basic client data in the BostonHMIS ("the warehouse"), in accordance with allowable uses and disclosures outlined in MA 66A to facilitate federal and state legal obligations. In addition, the HMIS data is covered by the protections outlined in the *Network Participation and Data Sharing Agreement* between the City of Boston and participating agencies. Clients may also choose to sign a Homeless Assistance Network Release of Information which gives permission for authorized personnel to view additional, more sensitive client data.

PROCEDURE

The data in the BostonHMIS is personal data, collected from people in vulnerable situations. BostonHMIS System Administrators, CoC HMIS Representatives, CoC Administrators, the HMIS Lead, and Authorized Agencies are ethically and legally responsible to protect the confidentiality of this information. The BostonHMIS will be a confidential and secure environment protecting the collection and use of client data. BostonHMIS and its partner agencies will ensure clients are informed of their data privacy and security rights through a tiered privacy policy that informs from the beginning of data collection through to the use and disclosure of data for the purposes of providing and coordinating housing and services.

Each Authorized Agency shall take appropriate steps to ensure that authorized users only gain access to confidential information on a "need-to-know" basis in accordance with this document and their own Privacy Policy. Duly authorized representatives of Boston's CoC, Collaborative Applicant, and HMIS Lead may inspect client records (including electronic records) at any time, although non-BostonHMIS staff will not, as a matter of routine, be permitted to access protected private information. BostonHMIS System Administrators, CoC HMIS Administrators, the HMIS Lead, and Authorized Agencies will ensure the confidentiality of all client data as described in this document.

II. Purpose and Use Limitations

POLICY

Agencies may use or disclose personally-identifying information from HMIS under the following circumstances: (1) To provide and/or coordinate services to an individual or household; (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 personal identifying information.

PROCEDURE

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 City of Boston Mayor's Office of Housing 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

III. Confidentiality

POLICY

Each agency must develop and implement written procedures to ensure: (1) All records containing protected identifying 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 the 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 pre-existing privacy policy of the recipient or sub-recipient and consistent with State and local laws regarding privacy and obligations of confidentiality.

IV. Protections for Victims of Domestic Violence, Dating Violence, Sexual Assault, and Stalking

POLICY

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 personal identifying information of the potentially dangerous circumstances that may be created by the improper release of this information.

V. Client Rights and Confidentiality of Records

POLICY

Clients may request to view or receive a copy of their information in the HMIS. However, data in the BostonHMIS is a reflection of the data input by the originating agency's(ies's) front-end system(s). Requests to amend, change, or de-identify their information must be made to the originating agency for resolution.

PROCEDURE

A client may request to view or receive a copy of their information from the HMIS by submitting a request through the HMIS Helpdesk.

VI. Agency Privacy Policy Requirements

POLICY

Each agency contributing data to the HMIS is required to provide information to the client related to the allowable uses and disclosure of their PII. An Agency's privacy policy and procedures must be in alignment with the HMIS Policies and Procedures and may not impede the HMIS Lead's ability to fulfill its legal obligations related to data. Clients have a right to be fully informed of their privacy rights as well as to review and amend or correction of their data, provided such requests are conducted per the privacy policies and procedures. Clients have a right to expect adherence to a high level of confidentiality of their information within the allowable uses and disclosures. To ensure compliance, agencies must implement the following data privacy procedures.

PROCEDURE

Agency Privacy Policy

Each agency contributing data to the HMIS is required to have a current privacy structure that includes, as a minimum:

- A privacy notice (see HUD's template here)
- A procedure for intake staff to follow to inform clients about their data privacy rights
- A policy related to Client Opt-Out to Sharing PII
- A policy and procedures for client requests to view, change/amend data, or delete/de-identify data

- A policy for client grievances
- A privacy toolkit for distribution to clients requesting any of the above
- A training schedule for staff on privacy and confidentiality
- Staff Accountability Requirements
- Policy and Procedures for Changes to Privacy Notice

Privacy Notice

Each Participating Agency is required to post a sign about their privacy policy in a place where clients may easily view it (i.e., at the point of intake - on a clipboard for outreach providers, in a case management office, an agency website, if they have one) and in languages appropriate to the clientele. The privacy posting must include:

- An explanation of personally identifying information
- A statement about the uses and disclosures of client data as outlined in this document.
- A statement of implied consent per the allowable uses and disclosures regulation in Massachusetts 66A.
- An explanation of the HAN Release and its opportunities for access to housing.

Intake Procedures

Each participating agency must have a written process for intake staff to follow to inform clients of their data privacy rights. This must be available for review during CoC Program, ESG, and HMIS Monitoring. The process must clearly articulate the information the intake staff will provide, when, and in what formats. The intake process must include, at a minimum:

- An explanation of the HMIS and the terms of consent to the client, including an explanation of how the information will be used, that the information is shared in the protected Network, and advantages of providing accurate information. Suggested documentation includes the BostonHMIS Client Info Sheet and the yoBostonHMIS Client Disclosure Sheet.
- A statement that clients cannot be denied services if consent to data collection is not given.

Client Opt-Out to Data Sharing of PII

Clients have the right of refusal to provide personal identifying information(PII) to the BostonHMIS. Clients may opt out of sharing PII during the intake process. When a client exercises his/her right of refusal, their information will be de-identified (made anonymous) at the data source before being provided to BostonHMIS.

If a client consents to data sharing of PII but later chooses to revoke their consent, the revocation will only apply to data collected after the revocation and will not retroactively affect previous data for which there was consent.

In these cases, it will be the responsibility of the CoC to provide alternative methods to capture the information outside of the HMIS system.

Such refusal or inability by the client to provide the information shall not be a reason to deny eligibility or services to a client.

Client Requests to View, Amend, or Delete PII

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 the correction of inaccurate or incomplete information about the individual but are not required to remove any information. However, the agency may mark information as inaccurate or incomplete and may supplement it with additional information.

Because of a legal obligation to collect data related to client use of housing and services to the U.S. Department of Housing and Urban Development as well as other federal, state, and local funding, a client's record cannot be deleted from the HMIS. In addition, a valid client record pertaining to the HMIS cannot be deleted from the original data source. If a client requests a record be deleted, it must be made anonymous in both the original data source and the HMIS.

An agency may deny access to a client's record for any of the following reasons, and should describe any other possible reasons in its Privacy Notice:

- Information compiled in reasonable anticipation of litigation;
- Information about another individual;
- Information obtained under a promise of confidentiality if disclosure would reveal the source of the information; or
- 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.

The agency must have written procedures that clearly articulate the process for a client to request a viewing of, changing/amending, or deleting/de-identifying their records. These procedures must include how the client can obtain and submit the proper forms and assistance in completing them, who the access authorizing person(s) will be for approving and managing the client request and access, the process for providing the client with access to or copies of their records, and resolution and documentation requirements, and timelines related to each step.

Client Grievances

Clients must be provided with a process to resolve issues related to their data if the agency cannot, or chooses not, to approve a client request for viewing, receiving copies of, changing/amending, or deleting/de-identifying their information. Each Authorized Agency is responsible for answering questions, complaints, and issues from their own clients regarding the BostonHMIS. Agencies must have a written procedure for managing client grievances. This procedure must include:

- A description of the process for the client to place the grievance (within the agency)
- A description of how to obtain and submit the proper forms and assistance in completing them (within the agency)
- what the grievance procedures and process is (within the agency)

- a policy and procedures for an appeal process (within the agency)
- a description of an escalation process (to BostonHMIS)
  - a description of conditions under which an escalation can be made (to BostonHMIS)

Client Grievance Escalation Process

Clients must contact the Authorized Agency with which they have a grievance for resolving of BostonHMIS problems. Authorized Agencies will report all BostonHMIS-related client grievances to the respective CoC Representatives, who in turn, will report these grievances to the BostonHMIS Lead Staff. If the Authorized Agency's grievance process has been followed without resolution, the Authorized Agency may escalate the grievance to the respective Boston CoC Representative as outlined in the "Authorized Agency Grievances" section.

Each Authorized Agency is responsible for answering questions, complaints, and issues from their own clients regarding the BostonHMIS. Authorized Agencies will provide a copy of their privacy policy upon client request. Client complaints should be handled in accordance with the Authorized Agency's internal grievance procedure and then escalated to the appropriate CoC Representative in writing if no resolution is reached.

The BostonHMIS Lead Staff is responsible for the overall use of the BostonHMIS and will respond if users or Authorized Agencies fail to follow the terms of the BostonHMIS agency agreements, breach client confidentiality, or misuse client data.

Authorized Agencies are obligated to report all BostonHMIS-related client problems and complaints to their CoC Representative, who will determine the need for further action. Resulting actions might include further investigation of incidents, clarification or review of policies, or sanctioning of users and Agencies if users or Agencies are found to have violated standards set forth in BostonHMIS Agency Agreements or the Policies and Standard Operating Procedures Manual. If a client requests that their data is no longer shared, the agency will have the client sign an updated Client Data Sharing Opt-Out form that will be retained in the client's file and change their sharing restrictions to Restrict to Org or Restrict to Basic Demographic Only in the HMIS system.

Client Data Request/Grievance Toolkit

Agencies must provide upon request to a client a toolkit that provides information on the privacy policies, client rights, policies and procedures for requests and escalations, any forms that must be completed, and timelines for each step for each type of request. These toolkits must be available in easily accessible formats for the client and in languages best fitting the client's needs.

Training Requirement

Agencies must ensure that staff is completing training on privacy and confidentiality on a yearly basis, minimally. Agencies must retain evidence of a staff's completed training and must be able to provide this evidence during monitoring.

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. Agencies must establish a written policy for accepting and considering questions or complaints about their privacy and security policies and practices.

Changes to Privacy Notice

Agencies must include in their privacy notice a statement that privacy policies and procedures are subject to change. If the agency has a process for identifying and making changes, it should be stated. The agency should identify the avenues and methods it will use to make known any privacy notice changes. Changes to Privacy Notice statements should not imply that clients will be directly notified of changes, even if the client is actively receiving services.

VII. Authorized Agency Grievances

POLICY Authorized Agencies will contact the BostonHMIS System Administrators to resolve BostonHMIS problems including but not limited to operation or policy issues. If an issue needs to be escalated, the BostonHMIS System Administrators may contact

BostonHMIS Lead Staff for further guidance. The BostonHMIS Lead Staff and the CoC HMIS Steering Committee will have final decision-making authority over all grievances that arise pertaining to the use, administration, and operation of the BostonHMIS.

PROCEDURE Users at Authorized Agencies will bring BostonHMIS problems or concerns to the attention of their Agency Administrator. If problems, concerns, or grievances cannot be addressed by the Agency Administrator, the Agency Administrator will contact their respective CoC HMIS Representative, who may ask for these issues to be stated in writing. If the grievance requires further attention, the BostonHMIS Lead Staff may consult with Boston's legal counsel. The Boston HMIS Lead along with the BostonHMIS Steering Committee shall have final decision-making authority in all matters regarding the BostonHMIS.

VII. Working Remotely

POLICY Agencies and Users are both responsible for maintaining client data security and privacy whether working in an office or remote. Sensitive Client data should never be left visible for unauthorized individuals to see or access.

PROCEDURE The following measures should be taken to prevent unauthorized viewing.

Wi-Fi/Software Protections

- Routers and Wi-Fi must be password protected with a secure password of at least 12 characters with a combination of numbers, lower-case and upper-case letters, and special characters.
- The computer in use must use anti-virus software that is up to date.
- Do not use public wi-fi connections, even if they are password protected.

Physical Location and Device Location

Users need to be aware of their surroundings and should consider the use of privacy screens. Ensure your screen cannot be seen by unauthorized persons.

- Devices must be set up in an area and at an angle so that personally identifiable data cannot be seen by unauthorized persons.
- Devices must be secure from theft.
- Ensure that all client identifiable data and access to ETO software or warehouse is removed or password protected from unauthorized persons.
- A password protected screen protector must be in use and set to 10 minutes

Use of Personal Computers

Shared computers should have a password protected account on the computer that is used only for work.

- Passwords are not to be stored in a place that is accessible by others.
- Password and screen protectors must be in use and set to 10 minutes
- All devices used in a remote setting must comply with all HMIS and CoC data privacy and security requirements
- All devices used in a remote setting must comply with all HMIS Policies and Procedures.

Downloading data to personal devices and storage options is not allowable. Downloads of data are only allowable to CHO or HMIS Lead owned devices and storage options.

V. Release of Data

Client Data Retrieval

POLICY Any client may request to view, or obtain a printed copy of, his or her own records contained in the BostonHMIS. This information should be made available to clients within a reasonable timeframe of the request. No client shall have access to another client's records in the BostonHMIS.

PROCEDURE A client may ask to see his or her own record. The Agency Administrator will verify the client's identity and print all requested information. The client may request changes to the record. The agency can follow applicable laws regarding whether to change information based on the client's request. A log of all such requests and their outcomes should be kept on file in the client's record.

The Massachusetts Statewide Data Warehouse

POLICY The state cannot transfer/copy the Boston CoC's data without prior written consent.

PROCEDURE The Department of Health and Community Development (DHCD) oversees the statewide data warehouse. To copy or transfer BostonHMIS data, DHCD must expressly request permission for each instance or through a legally binding contract/agreement that specifically addresses circumstances under which the state can transfer/copy data that belongs to the Boston CoC without their knowledge or consent.

Public Data Retrieval

POLICY The BostonHMIS Lead Staff will address all requests for data from entities other than Authorized Agencies or clients. No individual client data will be provided to any group or individual that is neither the Authorized Agency that entered the data nor the client himself or herself without proper authorization or consent.

PROCEDURE All requests for data from anyone other than an Authorized Agency or a client must be directed solely to BostonHMIS Lead Staff. BostonHMIS may also issue periodic public reports about homelessness and housing issues in the areas covered by the BostonHMIS. No individually identifiable client data will be reported in any of these documents.

Data Retrieval Support/Reporting/Media Use

POLICY Authorized CoC HMIS Administrators will create and run CoC- level and agency-level reports.

Authorized CoC HMIS Administrators and the System Administrators can create and execute reports on CoC –wide and agency-wide data, depending on their access level. This allows Authorized CoC HMIS Administrators to support CoC-level and agency-level goals.

PROCEDURE The CoC HMIS Administrators will be trained in the use of reporting tools by the System Administrator. The System Administrator will provide query functionality and templates for reports specifically for

BostonHMIS. The System Administrator may assist with the development of or running of reports/queries.

Research

POLICY

Agencies engaging research consultants or contractors, including research associated with state or federally-funded research efforts, must execute legally binding agreements with said consultants or contractors that include specific language binding them to compliance with all BostonHMIS policies and procedures.

Access to Data by Grant Funders

POLICY

The Mayor's Office of Housing (MOH) is responsible for the monitoring of recipient records and the evaluation of all programs and requires Contractor cooperation in the performance of these functions. MOH staff or designate(s) shall be allowed access to program staff, recipients, sites, books, documents, files, records, and papers of the Contractor which are pertinent to any matter covered in this Agreement. (MOH) will utilize agency data in aggregate or disaggregate form for, but not limited to, project plans, progress reports, financial records, invoices, supporting documentation, grant performance, or Homeless Management Information System (HMIS) compliance and problem resolution.

PROCEDURE

This policy applies to all grant recipients of MOH whose performance is subject to monitoring for compliance, progress assessment, and reporting purposes. A signed Release of Information form (ROI) from the client is required from the grant recipient or authorized representative. This form grants permission to access and review relevant records, documents, and information related to client enrollments, and grant recipient's project or activities.

Grant-related information obtained through the monitoring process is solely used for monitoring and evaluation purposes and is not disclosed or shared with any third parties unless required by law or authorized by the grant recipient. Information will be destroyed in accordance with current industry standards.

8. Data Security Requirements

I. Baseline Security Policy

Security standards ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users. Security standards must be followed by the HMIS Lead and participating agencies.

POLICY There are a number of state and federal regulations covering the release of client-identifiable data. The HUD HMIS Data and Technical Standards also specify minimum security requirements for the HMIS. Client identifiers include name, date of birth, and social security number, among others.

PROCEDURE The following protocols are to be followed to ensure the security of data entered into the HMIS:

1. All Users are issued a unique User ID and temporary password to access the system in accordance with Section 5.1 above.

2. All Users must sign confidentiality statements and attend training that includes information on data security.

3. Hard copies of data (if kept by the agency) must be stored in a locked file cabinet.

4. The HMIS Lead Agency shall be responsible for the destruction and disposal of its data, and each CHO shall be responsible for the destruction and disposal of its own data. Files must be disposed of appropriately in accordance with current industry standards after a minimum of 7 years, unless stored for research purposes (e.g., by cross-cut shredding of paper documents, magnetic swiping, and erasing and sanitizing electronic data in accordance with standards set out by the National Institute of Standards and Technology ("NIST")).

5. Computers must be set to lock after 10 minutes of inactivity and must be protected with a screen saver.

6. Computers are not to be left alone with PII data displayed.

7. After 3 failed log-in attempts, the User's password will be inactivated and they will be required to reset their password using the "Forgot Password" link.. Or, they may contact their System Administrator.

8. All data transmitted electronically must be encrypted (e.g., by encoding the data in such a way that only authorized parties can access it and those who are not authorized cannot). 9. Any data with PII stored on a device or external media (including removable devices, flash drives, and external hard drives) must be encrypted in accordance with the current industry standard.

II. Agency Requirements

POLICY An agency must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. 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.

III. End User Credentials

POLICY BostonHMIS/BostonClarity End Users will have access to each system via a username and password. Passwords must be changed a minimum of once every 120 days. Users will keep passwords confidential. Under no circumstances shall a user share a password, nor shall they post their password in an unsecured location; to do so will be considered a breach of the system user agreement. See section HMIS Policy Violations and non-compliance.

EXPLANATION Password integrity is a primary tool in ensuring system health, client data privacy, and blocking unauthorized access to client information. Therefore, under no circumstances is a username and password allowed to be shared in the BostonHMIS/BostonClarity live sites. In addition, usernames and passwords are not to be written or stored where they can be viewed by unauthorized personnel, clients, or visitors. For more information related to the protection of data and the system, please see the security section of this document.

PROCEDURE

Upon login with the username and temporary password, the user will be required by the software to select a unique password that will be known only to him/her. Every 90 days, end users will be prompted to change their password.

Strong passwords are critical to maintaining system integrity. The following requirements and restrictions help ensure that your password meets a minimum level of complexity.

Requirements

All passwords must contain at least:

- Eight characters or more.
- One uppercase character (A through Z).
- One lowercase character (a through z).
- One number (0 through 9).
- One non-alphanumeric character (!@#$()%^&*).
- No contain spaces.

Restrictions

No passwords may contain:

- The name of your Clarity Human Services instance.
- The word 'clarity.'
- Your First Name, Last Name, or Username.
- 'ABC' or '123.'
- More than two consecutive characters.
- The same password as the three prior passwords.

IV. Password Reset (Forgot Password)

Clarity Only

POLICY

Clarity Human Services users are able to change their password at any time by clicking their avatar or initials in the upper right corner and clicking *Account Settings*. In the event that a user has forgotten their password, they may click the "Forgot Password" feature on the Boston Clarity Live site login page.

PROCEDURE For Clarity HMIS, the system prompts you to enter the email address associated with your account. After you enter your email address, the system will display the following message: "We have received your request. If you are an existing user, we will send you an email with a link to reset your password."

Boston HMIS Data Warehouse

POLICY Warehouse users are able to change their password at any time by clicking 'Edit Account' in the Warehouse and clicking *Change Password*. In the event that a user has forgotten their password, they may click the "Forgot Your Password?" feature on the Boston Warehouse login page.

PROCEDURE For the Warehouse, changing password from the Edit Account page will require users to enter their current password and their new password twice in order to change. Using the 'Forgot Your Password?' feature, users will be required to enter the email address associated with their Warehouse account. Password reset instructions will then be sent to the email address provided.

ETO Software Systems

EA and Agency Managed ETO Software Systems should have similar processes and procedures in place to change the password of a user account. There should also be procedures in place for new training as needed when assuming new levels of access in the system.

Comparable Databases

Agency Managed Comparable Databases should have similar processes and procedures in place to change the password of a user account. There should also be procedures in place for new training as needed when assuming new levels of access in the system.

PROCEDURE The following protocols are to be followed to ensure the security of data entered into the HMIS:

1. All Users are issued a unique User ID and temporary password to access the system in accordance with Section 5.1 above.

2. All Users must sign confidentiality statements and attend training that includes information on data security.

3. Hard copies of data (if kept by the agency) must be stored in a locked file cabinet.

4. The HMIS Lead Agency shall be responsible for the destruction and disposal of its data, and each CHO shall be responsible for the destruction and disposal of its own data. Files must be disposed of appropriately in accordance with current industry standards after a minimum of 7 years, unless stored for research purposes (e.g., by cross-cut shredding of paper documents, magnetic swiping, and erasing and sanitizing electronic data in accordance with standards set out by the National Institute of Standards and Technology ("NIST")).

5. Computers must be set to lock after 10 minutes of inactivity and must be protected with a screen saver.

6. Computers are not to be left alone with PII data displayed.

7. After 3 failed log-in attempts, the User's password will be inactivated and they will be required to reset their password using the "Forgot Password" link. Or, they may contact their System Administrator.

8. All data transmitted electronically must be encrypted (e.g., by encoding the data in such a way that only authorized parties can access it and those who are not authorized cannot). 9. Any data with PII stored on a device or external media (including removable devices, flash drives, and external hard drives) must be encrypted in accordance with the current industry standard.

V. Security Officers

POLICY

The HMIS Lead must designate a HMIS Lead Security Officer. This Security Officer may be a member of the City's IT Department. The duties of the HMIS Lead Security Officer include, but may not be limited to:

- Review the Security Plan annually and at the time of any change to the security management process, the data warehouse software, the methods of data exchange, and any HMIS data or technical requirements issued by HUD. In the event that changes are required to the HMIS Security Plan, work with the HMIS and Data Committee for review, modification, and approval.
- Confirm that the HMIS Lead adheres to the Security Plan or develop and implement a plan for mitigating any shortfall.
- Respond to any security questions, requests, or security breaches to the BostonHMIS and communicate security-related HMIS information to participating agencies.

PROCEDURE

Each participating agency must designate a HMIS Security Officer; this person may also be the agency's HMIS Site Manager. The duties of the Agency's Security Officer include, but may not be limited to:

- Confirm that the agency adheres to the Security Plan or provide and implement a plan for mitigating any shortfall, including milestones to demonstrate elimination of the shortfall over time.
- Communicate any security questions, requests, or security breaches to the BostonHMIS System Administrator/Security Officer, and security-related HMIS information relayed from theBostonHMIS System Administrator to the agency's end users.
- Complete security training offered by the HMIS Lead.

VI. Annual Security Certification

POLICY

The HMIS Lead and each agency must complete an annual security review to ensure the implementation of the security requirements for the HMIS.

PROCEDURE

The 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. Each CHO Security Officer must complete the Security Self-Certification each January and submit the completed form to the BostonHMIS Administrator/Security Officer no later than February 1 of each year.

VII. Security awareness training and follow-up

POLICY

All users must receive security training prior to being given access to the HMIS.

PROCEDURE

The HMIS Lead has created an on-line security and privacy training module which must be completed prior to being issued a password. The request for a new password requires a certification that the new user has completed the on-line training. In addition, the HMIS Lead shall provide security training no less than once per year.

VIII. 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 suspected instances of noncompliance with these policies and procedures that may leave HMIS data vulnerable to intrusion. Each agency is responsible for reporting any security incidents involving the real or potential intrusion of the BostonHMIS to the HMIS Lead. The HMIS Lead is responsible for reporting any security incidents involving the real or potential intrusion of the BostonHMIS to the BostonHMIS Team.

Reporting Threshold

HMIS users must report any incident in which unauthorized use or disclosure of PII has occurred. Agency users will report any incident in which PII may have been used in a manner inconsistent with the BostonHMIS Privacy or Security Policies. Security breaches that have the possibility to impact the BostonHMIS must be reported to the BostonHMIS Administrator.

Reporting Process

HMIS users will report security violations to their agency HMIS Site Manager/ Security Officer. The HMIS Site Manager will report violations to the HMIS Lead Security Officer. Any security breaches identified by Green River will be communicated to the HMIS Lead Security Officer and System Administrator. The HMIS Lead Security Officer, in cooperation with the System Administrator, will review violations and recommend corrective and disciplinary actions to the HMIS and Data Committee and the Steering Committee, as appropriate. Each agency will maintain and follow procedures related to internal reporting of security incidents.

Audit Controls

BostonHMIS and BostonHMIS Clarity maintain an accessible audit trail that allows the BostonHMIS Administrator to monitor user activity and examine data access for specific users. The BostonHMIS Administrator will monitor audit reports for any apparent security breaches or behavior inconsistent with the Privacy and Security Policies outlined in these policies and procedures. In addition, Agency Site Managers are required to run audit reports on all HMIS user staff two times per year and submit these audit reports to the BostonHMIS Administrator.

System Security

POLICY Each agency must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, an agency"s networks, desktops, laptops, mini-computers, mainframes, and servers.

IX. By Name List

Access: The By Name List is only accessible to authorized Coordinated Entry Leadership, who can see and generate the list. The By Name List may be shared with scheduled, authorized case conferencing participants prior to the case conferencing meeting through protected conditions. A designated, authorized person will access or generate the By Name List for use at the case conferencing meeting. The authorized person will not share the by Name List with anyone other than the authorized, scheduled participants for the case conferencing meeting. The By Name List cannot be shared with anyone not part of the scheduled case conferencing meeting.

Protection: The By Name List contains PII. The By Name List may be downloaded for distribution to the scheduled case conferencing team as a password-protected Excel spreadsheet. Passwords will change for each scheduled meeting. Once password protected, the By Name List can be distributed to the scheduled, authorized case conference participants through encrypted email. Passwords for paper or electronic access to the By Name List must be treated in accordance with the password requirements in Section XXX. All paper and electronic participant versions of the By Name List must be properly disposed of after each case conferencing meeting.

9. Monitoring

I. HMIS Lead Monitoring

POLICY

The CoC Board and HMIS Policy group are jointly responsible for monitoring the HMIS Lead as defined in the governance charter. The HMIS Lead entity cannot monitor itself.

PROCEDURE

HUD has developed an HMIS Lead Improvement and Evaluation Matrix as well as other documents to help CoCs monitor the HMIS lead. These resources can be found on the HMIS Lead Series webpage.

II. Software Evaluation and Selection

POLICY

The United States Department of Housing and Urban Development (HUD) developed the data collection and reporting requirements for the Homeless Management Information System (HMIS) through the

2004 HMIS Data and Technical Standards Final Notice and subsequent updates to the HMIS Data Standards Manual, in collaboration with federal partners. The 2004 Technical Standards remain in effect, while the current Data Standards are updated periodically and provide the documentation requirements for the programming and use of all HMIS and comparable database systems. HUD requires that each Continuum of Care (CoC) designate a single HMIS for the geographic area and ensure that the HMIS is administered in compliance with requirements. However, HUD does not prescribe how an HMIS attains compliance with data and technical standards, or other required management and reporting capabilities as defined in the HMIS Data and Technical Standards, program-specific guides, and reporting specifications.

The HMIS Software Vendor Capacity Checklist provides CoC and HMIS leadership with a set of standardized criteria that the CoC may determine the HMIS Software Vendor should meet. These criteria generally are not to measure compliance, but rather to ensure that the HMIS Software Vendor provides software that meets the needs of the community. This checklist can also be used as a strategic planning resource for how HMIS can be used as a tool to prevent and end homelessness in the community.

Comparable Database Considerations:

What is a comparable database? A comparable database is a relational database that meets all HMIS Data Standards and the minimum standards of HMIS privacy and security requirements, including HUD's most recent reporting standards and comma-separated value (CSV) format specifications. A relational database is a collection of information that organizes data points with defined relationships for easy access and reporting. Excel and Google Sheets (spreadsheets) are not relational databases and do not meet the standard to be considered comparable in nature. It is important to select a comparable database that meets these requirements and identify it in any procurement or monitoring of Federal funds. Software that does not meet the baseline comparable database requirements will not be able to fulfill the management and reporting requirements that are required of Federal Funding recipients and sub-recipients. Working with your HMIS Lead on the selection of a comparable database can help provide insight into data management and reporting needs necessary to meet minimum standards.

PROCEDURE As a Government entity, the City of Boston Mayor's Office of Housing utilizes a public Request for Proposals in accordance with Massachusetts Procurement Laws for the procurement of services, supplies, and real property. Included in the RFP are requirements to maintain compliance with all federal rules, regulations, and requirements for data collection and reporting utilizing the HUD-provided HMIS Software Vendor checklist and other available HUD HMIS resources.

Organizations that decide to utilize their own agency-contracted software system or a comparable database must also utilize the checklists to confirm the software's ability to maintain compliance with the requirements.

III. Agency Monitoring

POLICY HMIS System Administrators will also have the right to conduct monitoring of CHO and User compliance with the policies and procedures detailed in this document.

PROCEDURE The HMIS Monitoring will be part of the CoC program-funded annual monitoring. The CHO will complete the HMIS Program Monitoring section of the Boston CoC Provider Self-Assessment Report. The HMIS monitoring consists of reviewing CHO's HMIS user activity, case file review, and an Assessment checklist.

CHOs will submit an applicable Annual Performance Report and HMIS Data Quality Tool Report from the Warehouse with the Self-Assessment Report, and in-person monitoring will also be conducted.

If the CHO does not pass their HMIS Monitoring, a corrective action plan will be developed between the CHO and the HMIS Lead. The

CHO will complete the corrective action plan within 90 days of receipt from the HMIS Lead. The HMIS Lead Agency may periodically review CHO for user compliance with Policies and Procedures and assist, where practical, with technical support to help such CHO comply.

Victim Service Providers are responsible for following this policy. No client-identifying information will be reviewed during the monitoring. All requested reports will be in aggregate form.

10. Data Security - Infrastructure

POLICY

The HMIS Vendor is obligated to maintain the security, performance, and support of the database system. To meet these requirements, the vendor must comply with the following procedures.

PROCEDURE

Vendor will comply with the following requirements to ensure optimal operation of the system.

Physical Security - Access to areas containing HMIS equipment, data, and software will be secured.

Firewall Protection - The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

User Authentication- Users may only access HMIS with a valid Username and password combination that is encrypted via SSL for internet transmission to prevent theft. If a User enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security -HMIS Users will be assigned a system access level that restricts their access to appropriate data.

Database Security -Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Technical Support- The vendor will assist HMIS staff to resolve software problems, making necessary modifications for special programming, and will explain system functionality to HMIS staff.

Technical Performance -The vendor maintains the system, including data backup, data retrieval and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

Hardware Disposal -Data stored on broken equipment or equipment intended for disposal will be destroyed using industry-standard procedures.

Database Integrity

The agency must not intentionally cause corruption of the BostonHMIS 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 agency, and suspension of continued access to the BostonHMIS by the agency.

The city 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 Section 4 of this Manual. An individual user may be subject to disciplinary action by the employer agency.

Data Storage and Transfer

Data extracted from the database and stored locally will be stored in a secure location (not on DVDs/CDs or other temporary storage mechanisms like flash drives or on unprotected laptop computers, for example) and will not be transmitted outside of the private local area network unless it is properly protected via encryption or by adding a file-level Password.

The BostonHMIS Administrators will provide help in determining the appropriate handling of electronic files. All security questions will be addressed to the BostonHMIS Administrators via the HMIS Helpdesk. Breach of this security policy will be considered a violation of the user agreement, which may result in personnel action and/or agency sanctions.

Hardware Disposal

Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures.

11. Disaster Recovery

POLICY

The HMIS software vendor provides disaster recovery services. The basic Disaster Recovery Plan includes the following (language provided directly from Bitfocus):

PROCEDURE

Contract will be reviewed upon each renewal to ensure disaster recovery options are outlined. HMIS Lead Agency will monitor the HMIS implementation health and coordinate directly with the vendor in the case of unexpected outages or disaster-related impacts.

Organizations that maintain a software system that is not contracted by the HMIS Lead must due their own due diligence with the chosen vendor.

12. Comparable Database Requirements

POLICY

Victim Services Providers (VSP) that are recipients or sub-recipients under the U.S. Department of Housing and Urban Development (HUD) Continuum of Care (CoC) and Emergency Solutions Grant (ESG) Programs are required to collect client-level data consistent with Homeless Management Information Systems (HMIS) data collection requirements. Violence Against Women Act (VAWA) and the Family Violence Prevention and Services Act (FVPSA) contain strong, legally codified confidentiality provisions that limit Victim Service Providers from sharing, disclosing, or revealing victims' personally identifying information (PII), including entering information into shared databases like HMIS. To protect clients, VSPs must enter required client-level data into a database that is comparable to and complies with all HMIS requirements.

PROCEDURE

Victim Services Providers (VSP) and the Boston CoC HMIS Administrators will use the HMIS Comparable Decision Tree to determine if the VSP is required to use a Comparable Database for data collection.

If a Comparable Database is required, the VSP will select a Comparable DB vendor and work with them to ensure the software complies with HUD's standards for a Comparable Database. The Comparable Database must be able to collect all fields (data elements) required for an HMIS by the kind of project it is (e.g., Emergency Shelter, Rapid Re-housing). It must also allow the user to enter specific data at multiple data collection stages (record creation, project start, status update, annual assessment, and project exit) to support reporting and performance measurements required by HUD for all CoC and ESG program recipients and sub-recipients.

All VSPs will follow the guidelines of the HUD Data Standards and the HUD Comparable Database Program Manual. They will be responsible for submitting their own Annual Performance Report (APR), Consolidated Annual Performance and Evaluation Report (CAPER), and data quality reports. The reports will be submitted in aggregate format.

As referenced in the Software Selection section, VSPs must utilize the HMIS Software Vendor Checklist to confirm that the chosen software vendor can maintain compliance with requirements.

13. Appendices

List of documents referenced that are not linked or public:

Agency Agreement

Boston HMIS Clarity End User Agreement

Boston Homeless Assistance Provider Network

Homeless Assistance Network Agreement (HAN)

BostonHMIS Warehouse User Agreement

Client Disclosure and Privacy Notice

Posted Privacy Notice Template

Data Quality Improvement Plan

User Access Role Matrix

Terms and Definitions

Data Collection Elements