Homeless Management Information System
Policies and Procedures

Mayor's Office of
Homeless Services

Most recent Data & Performance Committee Approval Date:
August 15, 2023

Baltimore City Homeless Management Information System
Policies and Procedures

Version and Review History

Date	Description
May 2, 2011	Initial Version.
September 11, 2012	Minor revision to the Laptop User Agreement.
August 2013	Major revisions were completed throughout the document.
December 2013	Minor revisions were completed throughout the document.
May 2016	Major revisions we completed throughout the document
August 2016	Major revisions were completed throughout the document
August 2017	Changes were implemented to the document including: 1. Participating agency and voluntary participation policies were merged to create one participating agency policy (2.1) 2. "Transfer of Data for purposes of Reporting" policy (1.3) added to clarify data sharing procedures for grant-required sharing. 3. "Affiliated Databases" policy was renamed to "Data Sharing with Affiliated Databases and Third Parties" (1.4). This policy was expanded to include data sharing, matching and transfers. 4. Added HMIS Lead monitoring to Data & Performance Committee Key roles and responsibilities (2.2) 5. Refined language in HMIS Lead Responsibilities (2.3) 6. Modified "Authorized Data Disclosure" (7.2.2) policy to be consistent with 1.3 and 1.4. 7. Interagency Sharing (7.3) policy Basic Sharing elements revised to be consistent with privacy policy. 8. Revised Data Quality Plan (8) to be consistent with monitoring plan and to clarify language. Added Bed data to Completeness. 9. Provider Monitoring Procedures (9) added.
November 29, 2017	Adjustments made to section 2.4 Procedures to reflect pre-screen process for data requests.
January 17, 2018	Adjustments made to section 2.1 Procedures to reflect implementation of HMIS Access request form and Committee approval process.
August 2018	Changes were implemented to the document including: 1. 1.2 Key terms: Clarified language regarding HMIS Lead Agency and HMIS Participating Agency responsibilities. 2. 1.3 HMIS Governance Amendment Process: Clarified language. 3. 2.1 Participating Agencies: Updated definition of HMIS Participating Agency with language used in HUD 2004 HMIS Technical Standards definition of "Covered Homeless Organization."

	4. 2.3 Report Requests: moved location in document. 5. 3.3 HMIS Lead Agency Responsibilities: Added Vendor relationship management responsibility and Board/Committee directive response procedures. 6. 3.4.2 HMIS Representative Responsibilities: Clarified responsibilities around reporting, data quality, and User Group Participation 7. 3.4.3 Agency HMIS Power Users: Added language to recommend when Power Users should be designated 8. Security Officer: Removed term "Security officer" from throughout the document and designated specific roles as responsible for responding to security incidents. 9. Agency Support Requests: added procedure for low help desk coverage. 10. Training: Added procedures for virtual training format. 11. 8.14 Security Incidents: Added detailed procedures for HMIS Participating Agencies and HMIS Led to respond to Security Incidents. 12. 9. Privacy Plan & Policies: Clarified language to align with HUD Technical standards requirements for Privacy Plan. 13. 10 Data Quality Plan: Updated section to add procedures for using Data Quality report cards to monitor data quality plan. 14. 11. HMIS Data Quality Report Cards: Added section. 15. 12. HMIS Participating Agency Monitoring: Updated Monitoring rates and frequency.
August 2019	Policy reviewed, no changes.
August 2020	1. Monitoring was updated to reflect temporary suspension of on-site monitoring due to COVID-19.
August 2021	Policy reviewed, no changes.
August 2023	Policy reviewed, no changes.

Background and Overview

1.1. HMIS overview

The McKinney-Vento Homeless Assistance Act, as amended by the Homeless Emergency Assistance and Rapid Transition to Housing Act of 2009 (HEARTH Act), requires that HUD ensure operation of, and consistent participation by, all recipients and sub recipients of funds in a community-wide Homeless Management Information System (HMIS). The HMIS has many uses. Some of the purposes of the HMIS, as established by the McKinney-Vento Act, include:

1. Collecting unduplicated counts of individuals and families experiencing homelessness
2. Analyzing patterns of use of assistance provided in a community
3. Providing information to project sponsors and applicants for needs analyses and funding allocations

The HMIS is also essential to coordinate client services, support performance management in the CoC, ensure accountability in the use of public funds, and to inform public policy.

The HMIS Lead Agency for the Baltimore Continuum of Care (CoC) is the Mayor's Office of Homeless Services (MOHS). In addition to administering the HMIS software, the HMIS Lead is responsible for maintaining the *HMIS Policies and Procedures* manual and all related documents, training system users, and providing help desk services. The HMIS Lead also monitors system users' compliance with policies and procedures.

The work of the HMIS Lead is overseen by the Baltimore City Data and Performance Committee. The Data and Performance committee is responsible for setting priorities, approving policies, and monitoring the work of the HMIS Lead. The Committee reports to the Journey Home Board.

Starting in 2013, the HMIS software provider for Baltimore City is ClientTrack Inc. Accordingly, in some parts of this document, the HMIS system is referred to as "ClientTrack."

1.2. Key Terms

1. Client- a person who receives services at an HMIS Participating Agency.
2. Exempt Agency- any organization that is required to report data on services provided to persons experiencing homelessness, but is exempt from entering that data into the HMIS by federal regulations.
3. HMIS Lead Agency (also referred to as "HMIS Lead") - the organization that oversees the administration of the HMIS. Within this document, responsibilities assigned to the "HMIS Lead" will be fulfilled by HMIS Agency staff at the discretion of the HMIS Lead manager, unless otherwise specified.

4. HMIS Participating Agency- any organization that utilizes the HMIS. Responsibilities or tasks referenced to be carried out by the HMIS Participating Agency will be fulfilled by the HMIS Representative, or assigned to stakeholders within the HMIS Participating Agency at their discretion, unless otherwise specified.

5. Coordinated Access - Baltimore City's system for ensuring coordinated access to all homeless services programs, including emergency shelter, transitional housing, rapid re-housing, and permanent supportive housing.

6. Coordinated Entry SSO (Supportive Services Only) Projects- Projects with dedicated funding to provide direct services to clients enrolled in or seeking access to Homeless Services Programs.

7. Community Matcher - The Community Matcher is the entity responsible for carrying out Coordinated Access matching policies and procedures in the Coordinated Access system, including but not limited to matching clients to vacancies following the Coordinated Access Prioritization Policy and troubleshooting the Coordinated Access system. The Community Matcher in Baltimore City is currently the Continuum of Care's Collaborative Applicant.

1.3 HMIS Governance Documentation Amendment Process

The Data and Performance Steering Committee and the HMIS Lead will guide the amendment of these *Policies and Procedures* and other HMIS governance documentation. The Data and Performance Steering Committee will review and recertify the *HMIS Policies and Procedures* and *HMIS Data Quality Plan* at least once annually and as changes are proposed.

Procedures:

1. Proposed changes may originate from any participant in HMIS, including clients.

2. When proposed changes originate within a Participating Agency, they must be reviewed by the Executive Director/ Program Director (or equivalent) of the Participating Agency and then submitted by the Executive Director/ Program Director (or equivalent) to the HMIS Program Administrator. Requests can be submitted to HMIS@baltimorecity.gov.

3. The HMIS Program Administrator will maintain a list of proposed changes.

4. The list of proposed changes will be discussed by the Data and Performance Steering Committee at least quarterly. At this meeting, the group will determine if these changes require additional research and if so, they will create a plan for completing the necessary research and timeline for completion.

5. If changes do not require additional research or once this research is complete, then the steering committee will vote to adopt or reject the recommended changes

6. Changes approved by the Data and Performance Steering Committee will be made by the HMIS Program Administrator and sent to all HMIS Participating Agencies. Except as mandated by HUD 30 days' notice will be provided before any changes are required to be implemented.

7. The Executive Director/ Program Director (or equivalent) from each of the Participating Agencies shall have 10 working days from the delivery of the amended document to acknowledge receipt and any concerns with the revised *Policies and Procedures* (or other documents). The Participating Agency's Executive Director/ Program Director (or equivalent) shall also ensure the circulation of the revised document within their agency and compliance with the revised Policies and Procedures.

8. Trainings on changes to HMIS documentation will be incorporated into HMIS User Group Meetings or scheduled as needed.

2. HMIS Reporting, Access and Data Sharing

2.1 Participating Agencies

An HMIS Participating Agency is any organization (including its employees, volunteers, affiliates, contractors and associates) that records, uses or processes PPI on homeless clients for the Baltimore City HMIS under the requirements and restrictions of the Baltimore City HMIS Participating Agency Agreement. Participating Agencies may participate in HMIS to fulfil requirements of funding sources, or may otherwise participate on a voluntary basis.

The HMIS Lead strongly encourages projects that serve persons who are homeless or at risk of homelessness and are not required to participate in the HMIS to do so voluntarily. Having more providers in the HMIS creates the potential for:

- More effective coordination of client services through case management and referral information sharing;
- More accurate tracking of client returns to the homelessness prevention and assistance system;
- More accurate counts of homeless persons and system resources, which could be used to understand the gaps in the service system;
- Better data about community-wide needs, which can help guide advocacy efforts, policymaking, and funding allocations; and
- Better data about system outcomes, which can be used to guide service targeting and performance improvement efforts.

Procedures:

1. All organizations requesting access to HMIS will complete the HMIS Access request form.
2. Organizations that are required to participate by funding requirements or other contracts may be approved by the HMIS Lead without notification of the Data & Performance Committee.
3. Other requests to participate in HMIS will be screened by the HMIS Lead and referred to the Data & Performance Committee for consideration.
4. The Data & Performance Committee will consider the request, using the HMIS Access Request form to evaluate the decision. The requesting agency may be asked to present to the Data & Performance Committee.
5. The Data & Performance Committee will approve or deny the request by vote.

6. The requesting organization will be notified of the decision by the HMIS Lead.
7. All Participating Agencies must sign a Participation Agreement before HMIS Access is granted, agreeing to adhere to all HMIS Policies and Procedures, regardless of voluntary or mandated HMIS participation.

2.2 Data Access

The Participating Agency retains access over all information entered into the HMIS.

Procedures:

1. In the event that the HMIS system ceases to exist, Participating Agencies will be notified and provided reasonable time to access and save data on persons served by the Participating Agency. Thereafter, the information collected by the HMIS will be purged or appropriately stored.

2. In the event that the Continuum of Care selects a different organization to serve as the HMIS Lead, the current HMIS Lead will work with the CoC and new organization selected to transfer the custodianship of the data for continuing administration. In that case, all HMIS Participating Agencies will be informed in a timely manner.

Participating Agencies that utilize other databases to record client level data or are ceasing participation in HMIS are permitted to export their programs' data from the HMIS and upload these data into other databases.

1. Agencies who transfer data from the HMIS are responsible for adhering to federal, state and local privacy laws within their databases.
2. Agencies requesting a data transfer with client information from outside their organization must complete a formal MOU between the agency and the HMIS Lead. The Data and Performance Committee must approve the MOU.

The HMIS Lead will follow all archiving data standards established by HUD in notice, as well as any applicable Federal, state, territorial, local, or data retention laws or ordinances.

Once data is archived, current and former Participating Agencies may request a copy of their data from the HMIS Lead from the archive.

2.3 Report Requests

1. The general public can request reports for non-identifying aggregate and statistical data by completing a Report Request Form, detailing the purpose and parameters of the information requested.
2. All report requests will be approved on a case-by-case basis and fulfilled at the discretion of the HMIS Lead and/or the Data and Performance Committee. The HMIS Lead may bring requests to the Data and Performance Committee as needed.
3. Reporting on clients by Participating Agencies must follow the same HMIS Security and Privacy policies outlined in this document. Reports containing identifiable information may only be shared with authorized users or under an MOU following procedures in section 2.5. Data must be stored securely following the Secure Storage protocols outlined in this document.
4. Any requests for reports or information from an individual or group who has not been explicitly granted access to the Baltimore City HMIS will be directed to the Data and Performance Committee.

5. No individual client data will be provided to meet these requests without proper authorization.

2.4 Transfer of Data for the Purposes of Reporting

Transfer of aggregate data or client PII to secure data repositories may occur for the purposes of fulfilling funding requirements. The HMIS Lead is authorized to evaluate and enter data sharing agreements for the purposes of fulfilling funding agreements authorized by the Collaborative Applicant. These funding sources include, but are not limited to:

- HUD: Continuum of Care
- Emergency Solutions Grants
- Runaway and Homeless Youth
- Housing Opportunities for Persons With AIDS
- Projects for Assistance in Transition from Homelessness
- Supportive Services for Veteran Families
- State of Maryland

Procedures:

1. The HMIS Lead will evaluate data sharing requirements of new funding agreements and ensure security protocols for data transfer and storage maintain client privacy and confidentiality.
2. When necessary, the HMIS Lead will provide specific training to providers on completing data exports and uploads for reporting purposes, and secure handling of client data.

2.5 Data Sharing with Affiliated Databases and Third Parties

With the approval of the Data and Performance Committee, the HMIS Lead may enter into a Memorandum of Understanding with a third party to enable data sharing, matching or transfer to or from the HMIS to or from another secure, managed database, so long as doing so is in furtherance of any of the Authorized Uses of HMIS Data (see section on Authorized Uses).

Before approving an MOU, the Committee will review:

1. Purpose and intent of MOU
2. What data elements for which clients will be shared, by whom, with whom, how frequently, and for how long
3. Consent and security policies of affiliated database
4. Potential benefits of MOU to current or future clients through care coordination, enhanced data collection, and system integration
5. Potential risks or harms to current and future clients
6. Monitoring procedures for the agreement
7. Term of the agreement

MOUs will be kept on record by the HMIS Lead. All data sharing, matching or transfers and their purpose will be listed on the MOHS website. The link to the website will be included in the HMIS Privacy Notice and HMIS Client Consent form.

Procedures:

1. The requestor will complete a Baltimore City HMIS Data Sharing Request form to be pre-screened by the HMIS Lead. The HMIS Lead will evaluate the request for viability. If deemed viable, the HMIS Lead will present the request to the Committee
2. The Committee may review the request prior to the formation of a formal MOU to make recommendations
3. All drafted MOUs will be presented to the Data & Performance Committee at a public meeting by the MOU party
4. MOUs are required to undergo legal review to ensure all security regulations and policies are adhered to
5. The Data and Performance Committee and HMIS Lead will do their due diligence in reviewing the technical components of the data transfer and data warehouse to ensure security policies are met
6. All MOUs must be approved by the Data and Performance Committee by a majority vote
7. The Data and Performance Committee is responsible for the review of expired or renewal MOUs

3 Stakeholder Responsibilities

3.1 CoC Board Responsibilities include but are not limited to:

1. Designate an eligible applicant to serve as the HMIS lead and manage the system.
2. Work with the HMIS Lead to measure and monitor progress towards making homelessness rare and brief.
3. Designate a single information system as the official HMIS software for the CoC
4. Work with the HMIS lead to encourage city wide provider participation except as exempt by law.
5. Define the requirements of the HMIS lead in the Governance Charter and By Laws

3.2 Data and Performance Steering Committee Responsibilities:

1. Work with the HMIS Lead to measure and monitor progress towards making homelessness rare and brief.
2. Create, monitor and revise (as needed) system-level performance data metrics and benchmarks.
3. Create, monitor and revise (as needed) project-level performance data metrics and benchmarks.
4. Review at least annually and approve revisions to the *HMIS Policies and Procedures*, the *HMIS Data Quality Plan*, and other significant HMIS policy documents.

5. Work with the HMIS Lead to prioritize and provide direction to data projects and work plans. Work with the HMIS Lead to develop an agreed upon action plan and timeline to fulfil Committee directives.

6. Oversee monitoring of the HMIS Lead Agency on an annual basis.

3.3 HMIS Lead Agency Responsibilities

1. Report to the CoC Board and Data and Performance Committee on system-level and project-level progress toward making homelessness rare and brief.

2. Ensure the consistent participation of any non-exempt recipients of funding programs that require HMIS participation.

3. Facilitate the operation and activities of the Data and Evaluation Steering Committee

4. Develop and maintain *HMIS Policies and Procedures document, HMIS Security Plan*, *Participation Agreement*, *System User Agreement*, *System User Confidentiality Acknowledgement* and other HMIS documentation and guidance under the direction of the Data and Performance Committee.

5. Ensure that all non-exempt Participating Agencies have signed and are in compliance with the agency's *Participation Agreement*.

6. Monitor data quality and compliance with HMIS policies and security protocols both within the database and through site visits to participating agencies.

7. Assign staff to enforce and audit adherence to HMIS security protocols among participating agencies, and respond to HMIS security incidents. The primary contact for incidents will be the manager of the HMIS Lead or, in their absence, the executive leadership overseeing HMIS Unit activities.

8. Enforce HMIS security protocols, including coordinating responses to suspected violations of client security and confidentiality policies, and proper disposal of Personally Identifiable Information (PII).

9. Oversee the setup and ongoing administration of the HMIS software and provide training, technical assistance and support to HMIS users in alignment with the Agency Support Request policies.

10. Manage the contract and work with the HMIS vendor to ensure compliance with HMIS Technical Standards, data collection and reporting requirements, and HMIS Policies and Procedures. Work with HMIS vendor to ensure ongoing usability of the system, including, adequate concurrent user licenses for the Baltimore City HMIS user base.

11. Ensure compliance with HUD HMIS Data and Technical Standards

12. Oversee customization of HMIS database, including the development of custom reports, and interface enhancements.

13. Oversee the collection, analysis and presentation of HMIS data for reporting to federal, state and local governments, private entities, clients, and citizens.

14. Lead performance evaluation activities.

15. Write, submit, and administer the HMIS project grant.

16. Maintain up to date information about the HMIS on the Lead Agency's website

17. Work with exempt agencies to ensure they are up to date on required data collection and reporting requirements.

18. Respond to motions and directives from the Data & Performance Committee and CoC Board by jointly creating an action plan, which specifies deliverables to be implemented on a mutually agreed upon timeline.

In line with HUD's recommendations for HMIS staffing structures, the HMIS Lead Agency will seek to maintain a minimum HMIS support staff ratio of 1 support staff person per 100 users, via local staff or contracted consultant services.

3.4 Participating Agency Responsibilities

3.4.1 Agency Executive Leadership/Program Director Responsibilities

1. Sign the *Participation Agreement* and submit it to the HMIS Director.

2. Ensure agency compliance with the *Participation Agreement*, *System User Agreement*, *System User Confidentiality Acknowledgement,* and *HMIS Policies and Procedures.*

3. Designate one employee as the HMIS Representative and notify the HMIS Lead of this assignment.

4. Work with the HMIS Lead to resolve HMIS data quality and compliance issues.

3.4.2 Agency HMIS Representative Responsibilities

More than one HMIS Representative may be designated at an agency if more than one person has authority within their Participating Agency to fulfil this role. This role should be designated by executive leadership within the agency who oversees HMIS activities, and responsibilities of each Rep be specified to the HMIS Lead Agency.

1. Ensure compliance with *HMIS Policies and Procedures*.

2. Serves as the primary contact for all concerns related to HMIS privacy and security. Responsible for overseeing and ensuring that all HMIS security and privacy protocols are implemented within their organization.

3. Ensures that any agency-specific data security policies and procedures are communicated to the HMIS Lead.

4. Sends updated agency-specific data security policies and procedures to the HMIS Lead within 30 days of any changes.

5. Designates and remove agency HMIS system users.

6. Designates and removes HMIS System Users authorized to serve as the HMIS Power User.

7. Ensure compliance with the agency-specific data security policies and procedures.

8. Documents and investigate suspected violations of client privacy or data security policies.

9. Notify the HMIS Lead within 24 hours of receiving reports of suspected violations of client privacy and data security policies.

10. Notify the HMIS Lead of the Participating Agency's response to suspected violations of client privacy and data security policies.

11. Serve as the primary contact for reporting, data quality reviews, HMIS monitoring, and HMIS operations within the Participating Agency.

12. Maintains access to advanced HMIS features to assist in Project Set Up and User Management.

13. Attend HMIS User Group meetings or send a representative from their HMIS Participating Agency (this may be the HMIS Power User or another System User).

3.4.3 Agency HMIS Power User Responsibilities

Agencies may designate HMIS Power Users who can serve as an alternate contact for HMIS activities, specifically reporting, data quality reviews, monitoring and other HMIS operations. This is recommended for Participating Agencies with multiple HMIS projects, which may be supervised by different staff. HMIS Representatives my designate additional responsibilities to the Power User but must notify the HMIS Lead. Responsibilities include:

1. Serves as an alternate contact in each agency for all agency users for support in using the HMIS.
2. Provides additional system use training to agency users as needed.
3. Maintains access to advanced HMIS features to assist in Project Set Up and User Management.
4. Supports the HMIS Representative in some tasks as authorized by the HMIS Representative.

3.4.4 System User Responsibilities

1. Sign the *System User Agreement* and *System User Confidentiality Acknowledgement* and submit copies to the HMIS Lead.
2. Comply with all HMIS agreements, policies, and procedures.
3. Report suspected violations of client privacy and data security policies to the Agency HMIS Representative within 24 hours.
4. Provide feedback to user's agency HMIS Representative or the HMIS Lead regarding system bugs or defects and/or recommended improvements to the system to increase ease of use.

3.4.5 Exempt Agency Responsibilities

1. Utilize a comparable database to the HMIS.
2. Develop database policies and procedures that comply with federal HMIS regulations.
3. Submit policies and procedures to the HMIS Lead.
4. Ensure compliance with agency-level policies and procedures.
5. Report de-duplicated, de identified data to the HMIS Lead to meet any federal, state or local reporting requirements

4 System Requirements

4.1 Hardware, Software, and Network Requirements

Each Participating Agency is responsible for meeting the minimum hardware, software, and network requirements to access the HMIS, and for providing the necessary maintenance for continued HMIS participation.

ClientTrack is a web-based application that can be accessed on a computer or mobile device. In order to access the HMIS, a device must have the latest version of one of the following browsers:

1. Internet Explorer/Microsoft Edge
2. Firefox
3. Google Chrome
4. Safari

The device must also have a secure internet connection.

4.2 User Designation

1. Each Participating Agency is responsible for designating staff who require access to the HMIS.

2. In the HMIS database, system users shall be assigned workgroups based on the program types they need access to and their roles at Participating Agencies. Participating Agencies will notify the HMIS Lead of the need to change a user's assigned workgroups.

3. Participating Agencies will notify the HMIS Lead of the need to deactivate system users within 24 hours of termination of their service with the agency. Advance notification is preferred, especially in the case of agency-initiated terminations.

4. In emergency removal situations HMIS Representatives may change the password of any users for which they are assigned as Supervisor in HMIS.

Procedures (To Designate a New System User):

1. The Executive Director, or designee, of a Participating Agency will complete the *User Authorization and/or Removal Form* and submit it to the HMIS Help Desk.

2. The new system user will read the *HMIS Participation Agreement* and *HMIS Policies and Procedures*.

3. The new system user will complete the *System User Agreement* and *System User Confidentiality Acknowledgement* forms and complete Security Awareness and System Orientation training.

4. The HMIS Lead Agency will provide new user training and logon information to the system user.

Procedures (To Change a System Users' Workgroup)

1. The HMIS Representative of a Participating Agency will submit a request to the HMIS Lead to change the user's workgroup.

2. The HMIS Lead Agency will change the user's workgroup and send a confirmation email to the user and the person who made the request.

Procedures (To Deactivate a System User):

1. The Executive Director, or designee, of a Participating Agency will complete the *User Authorization and/or Removal Form* and submit it to the HMIS Help Desk.

2. The HMIS Lead Agency will deactivate the system user within 24 hours of receiving the request.

Procedures:

1. Participating Agencies can request training from the HMIS Lead regarding data transfers.

2. The HMIS Lead will coordinate this training with the Participating Agency.

5 Agency Support Requests

1. Participating Agencies can request HMIS technical support from the HMIS Lead through the HMIS Help Desk.

Procedures:

1. Support requests can be submitted by calling the HMIS Help Desk, Monday through Friday, 8:30am to 4:30pm, emailing the HMIS Help Desk or by submitting a support ticket within the HMIS Software.

2. All HMIS Support requests will receive a response in 24 business hours. If for any reason there is reduced coverage of the HMIS Help Desk that may result in a delayed response time, the HMIS Lead will communicate the term of the reduced coverage to HMIS users, either via email communication, help desk email auto-reply, voicemail message or other means.

5.1 System Customization requests

1. If, after implementation, the agency wishes to use HMIS for other project or make adjustments to current project configurations, the agency's HMIS representative must submit a written or electronic change request to the HMIS Lead Agency.

2. The Data and Performance Committee, shall review, request additional information and decide upon any requests based on evidence-based practices, consistency with other program types, and potential risks and benefits to current and future clients.

3. The Data and Performance committee will make recommendations to the CoC Board and HMIS Lead on improvements to the HMIS System.

Procedures:

1. Participating Agencies should complete the HMIS Enhancement Request form to submit any request for system customizations

6 Data Requirements

6.1 Minimum Data Requirements

1. Each Participating Agency is responsible for collecting the data elements required for their project type by their funding source(s), as specified by their contract, program regulations, and HMIS regulations and guidance.

2. Each Participating Agency is required to communicate to the HMIS Lead changes in funding sources or project definitions to ensure the maintenance of accurate data

3. For each client served, every Participating Agency is required to enter the minimum required data fields (i.e. entry, update, annual and exit assessments), related to the programs it is operating in. The entry should be entered into HMIS in a timely manner in alignment with the Data Timeliness standards established in the HMIS Data Quality Plan. Minimum HMIS Data requirements can be found in the HMIS Data Standards Manual.

6.2 Local Data Collection Policies

Housing Data Requirements

1. Each Participating Agency is required to maintain up to date Bed and Unit Inventory Information within HMIS in alignment with HMIS regulations and guidance

2. Data should be reviewed no less than annually and updated when inventory changes.

3. HMIS Representatives may maintain housing set up, or contact the HMIS Lead agency for assistance, specifying housing changes.

4. Each Non-Exempt Participating Agency funded by the HMIS Lead that provides shelter beds or housing is required to document Check-Ins and Check-Outs within HMIS.

5. Housing Check-Ins and Check-Outs should be entered into HMIS in alignment with the Data Timeliness standards established in the HMIS Data Quality Plan.

6. Residential Projects that want to use HMIS to track clients to whom they provide services that do not result in an overnight stay must have a separate project with a project type of 'Services Only' set up for this purpose.

Service Data Requirements

1. Each non-exempt Participating Agency is required to document within the HMIS services that are provided by the organization OR services that are required by their funding program (ex. RHY, SSVF, PATH) that are listed in the HMIS Program Manual.

2. HMIS Representatives should contact the HMIS Lead to ensure that the appropriate service codes are available for their organization.

Street Outreach Data Collection

1. Street Outreach projects are required to enter a client to their project within HMIS at the first contact with a client. An enrollment date is required, however an HMIS engagement date is not required until the client agrees to engage in services from the project.

2. Street Outreach projects are required to log all outreach contacts made before and after a formal engagement within HMIS.

3. Staff in Street Outreach projects should identify all clients in HMIS that need to be discussed at the weekly outreach coordination meeting.

4. When a client provides consent to engage in services from a Street Outreach project, an engagement date and required data must be entered into HMIS.

5. Clients are to be exited from the Street Outreach Project within HMIS when the client has been successfully transitioned to another HMIS project, the client has become inactive or is terminated from the project. Criteria for client inactive status or termination may be found in the Standards of Care. [Insert Link]

Procedures:

1. Enrolling Outreach Contacts:

    a. If the client chooses not to engage, using the Short Intake workflow and enter in as much information as can be gathered from the client.

    b. The Project Entry date is the date of the first Contact.

    c. For subsequent contacts, Street Outreach Projects should continue to enter information to the same intake record utilizing the “Edit Enrollment Workflow” function, until the point of engagement.

    d. Street outreach projects should develop and maintain an internal naming policy and system for tracking and updating aliases used during the Contact period.

        i. Until the point when a legal name is obtained, the alias should be entered into the Name fields on the Basic Information Form. If an alias is used in the Name fields, “Name Data Quality” should be entered as “Partial, street name, or code name.”

        ii. After the legal name is obtained, edit the Name fields to reflect the legal name, and enter the alias on the Client alias form.

    e. Due to the nature of outreach services, there may be duplicate client records for one person. When duplicate client records are identified during the weekly outreach coordination meeting (currently HIP) contact the HMIS Lead Agency with the alias and legal name information to merge these records.

f. At the point of engagement, Outreach Projects compete the client enrollment record in the project by completing the Full Intake workflow tied to the same enrollment.

g. The Project Entry date remains the date of the first Contact, regardless of whether the client fully engaged on that date.

h. The Date of Engagement field on the Program Enrollment form should reflect the date at which the client agreed to receive services from the project.

Note: Data quality for Street Outreach projects only applies to clients with an engagement date

Rapid Rehousing Data Collection

1. Rapid re-housing projects will follow the "Identifying Residential Move-In Date" method for entering a client into the Rapid Re-Housing project.

2. Clients are to be exited from the Rapid Re-housing project in HMIS when the client no longer receives services from the program and the case is formally closed. When a case is formally closed may be determined by projects to align with their internal case management practices. This may be when eligibility ends, or at some other point prior to eligibility ending.

3. Previously exited clients that return for services should receive a new enrollment into HMIS.

4. Rapid Re-Housing projects will enter Housing data for clients receiving Rental Assistance through the program for the purpose of tracking utilization.

Procedures:

1. Residential Move-In Date Method:

    a. The Project Entry Date is the date the person eligible for Rapid-Re-housing assistance is admitted to the project, even if only in initial stage of engagement. The project entry may be earlier than the client's move-in date

    b. At project entry, record the Universal Data Elements and all information required at project entry.

    c. When the client moves into housing, update the Residential Move-In Date field to reflect the date the client physically moved into the housing unit.

Homelessness Prevention Data Collection

1. Homelessness prevention projects must reevaluate and update as necessary information on Homelessness Prevention clients once every three months. Information required to be updated in the HMIS, if changes have occurred include:

    a. Income and Sources

    b. Non-Cash Benefits

c. Health Insurance

2. Clients should be exited from the Homeless Prevention HMIS project when eligibility ends or if the case is formally closed for another reason before the eligibility end date.

3. Homelessness Prevention projects are not required to maintain detailed records of financial assistance payments, such as payment amounts, within HMIS, however providers must log payments made to clients as a service.

Procedures:

1. An Update/Annual Assessment should be completed every three months following project entry.

7 Training Policies and Procedures

7.1 Training attendance

1. Successful completion of any in-person training requires full attendance during the training session. Successful completion of any virtual training requires full completion of all training components within the allotted timeframe.
2. For in-person training sessions, lateness of more than 10 minutes or departure more than 10 minutes prior to the end of the training will count as an incomplete training, and users will be required to repeat the training on the next available training date.
3. Absences or non-completion will be reported to the HMIS representative.
4. Depending on the nature of the training, non-attendance or non-completion may result in system access being revoked until the training requirement is fulfilled. Users and their HMIS representative will be notified if system access will be revoked due to non-attendance.

7.2 New User Training

1. New users must complete the HMIS New User Training and pass the Baltimore HMIS Basic User Certification test at the conclusion of each training. New HMIS Users will not be granted access to HMIS until the training and Certification test is successfully completed.
2. The Baltimore HMIS Basic User Certification test is administered during the HMIS New User Training and may be taken with the support of notes and consultation with the Trainer.
3. A user will have three attempts to pass the HMIS Basic User Certification test during the training period. If the user fails to successfully complete the test, the HMIS Lead Agency with the user's HMIS Representative will develop a remedial training plan and steps to gain system access.

Procedure: Registering a new user for Security Awareness and System Orientation Training

1. The HMIS Rep submits the completed HMIS New User Authorization form to the HMIS Lead Agency and 1) sends a request to the HMIS help desk to include the user in the next training or 2) registers the new user for the training.
2. HMIS Lead Agency sends a confirmation request to the trainee and the trainee confirms their attendance at least 48 hours before the training.

7.3 HMIS Representative Training

1. In addition to Security Awareness and System Orientation training, HMIS Representatives are strongly encouraged to attend an HMIS Representative Orientation session with the HMIS Lead or complete similar training if available. The orientation will review the HMIS Representative's roles and responsibilities, security protocols and advanced HMIS features.

7.4 Annual Refresher Trainings

1. All system users are required to attend an Annual Refresher Training session that will review new functionality, and updates to policies and procedures.
2. Annual Refresher Trainings are required once in a calendar year.
3. Additional trainings targeted to a specific user type, project type or other criteria may be required at the discretion of the HMIS Lead Agency, depending on the nature of updates to be reviewed.

7.5 Voluntary Trainings

1. Additional trainings and certifications on advanced HMIS functionality will be made available as staffing capacity permits and CoC needs dictate.

7.6 Training Information

1. HMIS Representatives may request a list of users and their most recent training dates at any time from the HMIS Lead.
2. Training information will be posted and maintained on the HMIS Lead website and communicated regularly to the HMIS Representatives and Power Users.

8 Data Security Policies

The security standards set in the 2004 Data and Technical Standards Notice (Section 4.3) serve as baseline standards adhered to by the Baltimore City CoC. These security policies described in this section are local policies meant to enhance further the security of information collected through HMIS. These security policies are directed to 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.

8.1 Security Management, Compliance and Review

1. The HMIS Lead Agency has responsibilities to manage the selection, development, implementation and maintenance of security measures to protect HMIS information.
2. The HMIS Lead Agency must retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or otherwise required.
3. The HMIS Lead Agency must complete an annual security review to ensure the implementation of the security requirements for itself and Participating Agencies, using a checklist to ensure compliance with each requirement defined in this section.
4. The HMIS vendor will track metadata on what a user has viewed in addition to what a user has edited, in case inappropriate use must be investigated.

8.2 Security Contact

1. A Participating Agency's HMIS Representative is expected to serve as the primary contact for all security incidents and is responsible for ensuring compliance with applicable security standards and protocols.
2. The HMIS Lead Manager, or, in their absence, the executive leadership overseeing the HMIS Lead, is responsible for ensuring compliance with applicable security standards and protocols.

8.3 Disaster recovery

1. The HMIS Software Vendor is required by contract to implement technical safeguards to prevent data loss in the event of a disaster. In such an event, the vendor will contact the HMIS Lead Agency and provide a timeline for recovery. The HMIS Lead Agency will then

communicate the timeline with other stakeholders, include instructions to guide operations during the recovery process, and provide periodic updates as well as notification upon successful recovery of any data loss.

8.4 Workforce Security

1. Participating Agencies are recommended to conduct criminal background checks or similar screening practices in accordance with their internal hiring practices on the HMIS Representative and on users with system access beyond their primary organization of employment.

8.5 Security Training

1. HMIS Lead Agency must ensure that all system users receive training on security policies and procedures within the HMIS New User Training before given access to the system and at least annually during HMIS Refresher Trainings. The HMIS Lead Agency will maintain attendance records for all training events to assure compliance. See section 5 for training-specific policies and procedures.

8.6 Device and Network Requirements

1. Participating Agencies and HMIS Lead Agency must ensure that devices used to access the HMIS have password-protected access with automatic system lock after no more than 15 minutes of user inactivity.
2. Participating Agencies and HMIS Lead Agency must ensure that computers used to access the HMIS have virus protection, in accordance with the agencies internal policies, that is updated at least annually.
3. Participating Agencies and HMIS Lead Agency must ensure that internet connections used to access the HMIS are set up using basic standard network security protocols to prevent unauthorized access to your network and to HMIS data stored in local servers or hard drives.

8.7 System Passwords

1. System users' passwords may not be shared, even among other authorized HMIS users.
2. System users may not allow an internet browser to save their HMIS passwords.
3. System users may not store their passwords in locations that are easily accessible to others (i.e. under the computer keyboard or posted near the workstation or on personal devices).

8.8 System Access Physical Location

1. Because of the confidential nature of data stored within HMIS, the system must be accessed from a sufficiently private physical location so as to ensure that persons who are not authorized users of the HMIS are not able to view client level data.
    a. Users must log out of the HMIS system when their work space will be unattended or accessed by unauthorized persons. The system will automatically logout a user after 15 minutes of inactivity.
    b. User must ensure screens and monitors used to access HMIS are not positioned so that non HMIS users may see information. Alternatively, monitor privacy screens must be used.

8.9 User Inactivity

1. User accounts that have not been accessed for 60 or more days will be automatically disabled, meaning the user will be unable to access the system.
2. User accounts that have not been accessed for 180 or more days will be automatically disabled and have their prior authorization invalidated, meaning the user will need to be reauthorized before they can access the system.

Procedure:

1. For accounts inactive for more than 60 days, but less than 180 days, HMIS Representatives must contact the HMIS Help Desk on behalf of a user whose account has been disabled after 60 days of inactivity, if the Participating Agency wishes to reactivate the account. The account will be reactivated at the discretion of the HMIS Help Desk.
2. For accounts inactive for more than 180 days, HMIS Representatives must submit a new HMIS user authorization request to the HMIS Help Desk for any inactive user that still needs access to the system. These re-authorized users will then need to retake the HMIS Basic User Certification test. Users have the option to attend Security Awareness and System Orientation training if desired.

8.10 Personally Identifiable Information (PII) Storage and Management

1. System users are responsible for maintaining the security of all client data extracted from the HMIS and any data collected for purposes of entry into the HMIS via methods that align with the HUD Data and Technical Standards (section 4.3.2 & 4.3.3)

8.11 Electronic Data Storage and Management

1. System users may only store HMIS data containing client level PII on devices owned by their agency.
2. System users may not store HMIS data containing client level PII on portable hard drives or removable media unless the file or device is password protected.
3. System users are responsible for safeguarding HMIS client level PII that users store on agency-owned devices.
4. Electronic transmission of HMIS data containing PII will be limited to secure direct connections or, if transmitted over the internet, the data will be encrypted using a 128-bit key or transmitted using password protected files.

5. Participating Agencies and HMIS Lead Agency are responsible for developing additional policies and procedures for protecting electronic data from theft, loss, or unauthorized access.
6. Before disposing of hard drives used to store PII, Participating Agencies will consult with the HMIS Lead.

8.12 Hard Copy Data Storage and Management

1. Hard copies of HMIS data containing PII shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, hard copies of HMIS data containing PII shall be maintained in such a manner as to prevent exposure of PII to anyone other than the system user(s) directly utilizing the information.
3. Employees shall not remove hard copies of HMIS data containing PII from their Agency's facilities without permission from appropriate supervisory staff unless the employee is performing a regular work function which requires the use of such records outside of the facility.
4. Faxes or other printed documents containing PII shall not be left unattended.
5. Before disposing of hard copies of HMIS data containing PII, they must be shredded.
6. Participating Agencies and HMIS Lead Agency are responsible for developing additional policies and procedures for protecting hard copies of HMIS data containing PII from theft, loss, or unauthorized access.

8.13 Agency Specific Data Policies and Procedures

1. Participating Agencies may develop agency-specific data security policies and procedures that go beyond the standard policies included in this section.
2. Participating Agencies are required to provide copies of agency-specific data security policies and procedures to the HMIS Lead if they are different from the HMIS Policy and Procedure's security policies. An updated copy of the agency-specific data security policies must be provided any time there is a change to the document.
3. The HMIS Lead is responsible for reviewing agency-specific policies and procedures to determine if they conflict with the *HMIS Policies and Procedures* and resolving any conflicts.
4. Participating Agencies are responsible for ensuring compliance with any agency-specific data security policies and procedures.

8.14 Reporting Security Incidents

1. A security incident is any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in the HMIS.
2. HMIS Participating Agencies are expected to develop and maintain procedures for investigating and resolving security incidents involving client-level data, including HMIS data. HMIS Participating Agencies are expected to provide copies of these procedures to the HMIS Lead Agency, and notify the HMIS Lead whenever changes occur.
3. Participating Agencies and HMIS Lead Agency will post a notice anywhere HMIS data is collected or accessed that articulates the reporting mechanism for suspected breaches of data security. The notice will include contact information for the agency's HMIS

Representative. The notice will include additional instructions for reporting anonymously.

4. Upon becoming aware of a suspected security incident, System Users must report the security incident to the HMIS Representative. A user may report any incident directly to the HMIS Lead Agency via hmis@baltimorecity.gov or 410.396.4647. If the security incident involves the HMIS Lead Agency, the user may report the incident to the Chair of the Data and Performance Committee.
5. A report of a security incident to an HMIS Representative should trigger the HMIS Participating Agency to follow their internal procedures for investigating a suspected security incident. If the security incident is confirmed to be a successful security breach, resulting in unauthorized use, disclosure, modification or destruction of HMIS data or interference with HMIS operations, the Participating Agency should notify the HMIS Lead.
6. In the event a security incident is reported directly to the HMIS Lead and/or the Data & Performance Committee, the HMIS Lead and/or Chair of the Data & Performance Committee will work with the appropriate parties to investigate the incident.
7. If the security incident resulted from a System User's suspected or demonstrated noncompliance with the System User Agreement or Confidentiality Acknowledgement, the HMIS Representative should request to have the System User's HMIS access deactivated until the investigation has been completed. The HMIS Lead Agency reserves the right to deactivate any system users suspected of unauthorized use or disclosure of HMIS data until an investigation has been completed.
8. In the instance of a confirmed security incident and dependent on the nature of an incident the HMIS Lead will develop a follow up action plan and timeline jointly with the HMIS Participating Agency. The development of this plan may involve additional parties at the discretion of the HMIS Lead Agency.
9. The HMIS Lead Agency will notify the appropriate body of the Continuum of Care of any substantiated release of PPI in noncompliance with the provisions of the HMIS Policies and Procedures, and/or the HMIS Privacy Notice.
10. Participating Agencies and HMIS Lead Agency will maintain records with the following information of all security incidents, responses and outcomes.
    - Date of incident
    - Individuals involved
    - Project(s) involved
    - Type of incident
    - Impact
    - Resolution
    - Date of Resolution

9 Privacy Plan & Policies -

9.1 Purpose Use and Limitations

The HMIS Lead and HMIS Participating Agencies may only collect and use HMIS data for the specific internal purposes and reasons relevant to the work of the Continuum of Care, as defined in the HUD Data and Technical standards, the HMIS Privacy Notice and this document. Every organization

with access to Personally Identifiable Information (PII) must implement procedures to ensure and monitor its compliance with privacy policies and may only collect information by lawful and fair means with the knowledge and consent of the individual.

9.2 Allowable uses and disclosures

9.2.1 Authorized uses of HMIS Data

1. To provide or coordinate services;
2. To locate programs that may be able to assist clients;
3. To refer clients to HMIS-participating programs;
4. To establish client eligibility for programs;
5. To produce agency-level reports regarding use of services;
6. To track agency-level and system-level outcomes;
7. For agency operational purposes, including administrative functions such as legal, audits, personnel, oversight, and management functions
8. To comply with government and other funding agency reporting requirements;
9. To identify service needs in our community;
10. To support system-level planning;
11. To conduct research for governmental and educational purposes approved by the Data & Performance Committee;
12. To monitor compliance with HMIS Policies and Procedures;
13. To further partnerships and initiatives entered into by the Baltimore City Continuum of Care.

9.2.2 Authorized Data Disclosures

1. Disclosures of client-level data may occur when required by funding, as outlined in section 2.3 or otherwise through a formal MOU developed by following the procedures outlined in section 2.4. Disclosures may occur without MOU when required by law (i.e. court order).
2. Aggregate data that does not contain any client specific identifying data may be shared with internal and external agents without specific permission if there is no reasonable basis to believe that it could be used to identify an individual.
3. Care Coordination and Case Conferencing - Data that is shared globally or with selected agencies in HMIS may be discussed in a case conferencing format as long as all participating organizations present have signed HMIS Participation Agreements.
    a. Any HMIS information shared in case conferencing beyond basic client information must have appropriate client consent.
    b. If an organization has not signed the HMIS Participation Agreement, additional consent must be obtained from any clients whose information will be shared.

9.3 Interagency HMIS Data Sharing

1. All information entered in the HMIS is shared with users within the agency who enter the information and the HMIS Lead Agency.
2. There are six types of consent used by homeless services providers in the HMIS system: no consent, inferred consent, verbal consent, signature, additional signature, and non-HMIS data

exchange (requires signature). See Types of Consent Table for details on when and how each consent type is used.

3. Certain information, when saved in HMIS, is always shared globally to prevent duplication of client records and services. These basic, globally-shared client information fields are listed in the *Client Consent to Share Information* form and include:
    - Name
    - Date of birth
    - Social security number
    - Race
    - Ethnicity
    - Gender
    - Sexual Orientation
    - Veteran Status
    - Disabling condition
    - Veteran challenge assessment
    - Client Contact Information
    - Family Contact Information
    - Emergency Contact Information
    - Household composition information
    - Urgent notifications
    - Street Outreach Enrollments and Contacts (among other Street Outreach providers)
    - Coordinated Access Status and Status History

4. Client level data collected by programs beyond the basic sharing elements listed above are shared with all HMIS participating organizations based on the individual client's preference as expressed on the *Client Consent to Share Information* form, excepting information that requires an additional signature for sharing
5. Client level data collected by programs, beyond the basic sharing fields listed in the HMIS *Client Consent to Share Information* Form, may be shared with all HMIS participating organizations only when the sharing agency has secured valid consent forms from the client authorizing such sharing and only during such time that the consent forms are valid (before their expiration, unless consent has been revoked earlier).
6. VSP Providers may obtain client consent to allow client information to be shared with the HMIS Lead and an HMIS participating agency upon transfer to an HMIS participating agency.
7. Each Participating Agency's Executive Director/ Program Director (or equivalent) is responsible for his/her agency's compliance with the Interagency Data Sharing Policies. Violation of these policies may result in suspension of system access.

9.3.1 Client Consent

1. By providing information to a Participating Agency, persons who receive services consent to having that information entered into the HMIS, and thereby consents to have all basic client information fields listed in the *Client Consent to Share Information* form shared with all HMIS

participating organizations (see section 5.5), and all information entered into the system shared within the organization that entered the information, and with the HMIS Lead Agency.

2. Clients who have consented to additional sharing of information may revoke consent in writing at any time using the *Client Consent Revocation* form. This revocation applies all information in the HMIS, including data collected at other Participating Agencies.

3. The *Client Consent to Share Information* form is valid for three years after signed.

4. In order to enable additional data sharing time, the *Client Consent to Share Information* must be completed annually.
5. Participating Agencies must maintain physical copies of client consent documentation for a minimum of seven years. For programs that were funded with Continuum of Care funds for the acquisition, new construction, or rehabilitation of a project site, client consent documentation must be retained until 15 years after the date that the project site is first occupied, or used, by program participants.

Procedures (Initial Consent):

1. During the first meeting with a client where HMIS or Coordinated Access data are gathered, a representative from the Participating Agency will notify the client that the information they collect will be entered into the HMIS, what HMIS is and will explain the purposes for collecting information in the HMIS.
2. During this meeting, a representative from the Participating Agency will explain the *Client Consent to Share Information* form, and the client's right to revoke data sharing in writing at any time.
3. Agency representatives have the following two options for obtaining informed consent from members of a multi-person household. The agency representative must choose between these options in consultation with the client(s). In some occasions, both options may be appropriate for one family, where some family members are included in one form, and others have their own separate form.
    a. An adult client can provide consent for members of his/her household that are minors by listing them in the spaces provided in the form and initialing in front of each family member's name.
    b. One consent form is completed for each individual in the household. A legal guardian (or another adult if a guardian is not present) may sign for minors in the household.
4. The client must sign the *Client Consent to Share Information* form as proof that they had an opportunity to review the form and get their questions about its content answered.
5. If the client signs the form and agrees to share additional information with all HMIS participating agencies, the Participating Agency representative must select "Yes" in the client consent drop-down menu on the Basic Client Information form in ClientTrack.
6. If the client indicates on the form that he/she declines to share additional information with all HMIS participating agencies, the Participating Agency representative must select "No" in the client consent drop-down menu on the Basic Client Information form in ClientTrack.

7. A copy of all completed consent forms will be kept in the client's paper file. These forms may be reviewed by the HMIS Lead during the annual security review.

Procedures (Revocation of Consent):

1. If a client presents a written request to revoke consent for information sharing in the HMIS, a Participating Agency representative must store the written request in the client's file, and will select "No" in the client consent drop-down menu on the Basic Client Information form in ClientTrack.
2. If a client verbally requests to revoke consent for data sharing, Agency Representatives must ask the client to complete the *Client Revocation of Consent to Share Information* and follow the process specified in (1) above.
3. A copy of all written Revocation of Consent requests must be included in the client's paper file.

Procedures (Renewal of Consent):

1. Prior to the expiration of a client's' existing *Client Consent to Share Information*, the Participating Agency must request the client to complete a new *Client Consent to Share Information* form.
2. Agency Representatives must follow the same procedures that were specified above involving the completion of the initial consent form.

9.4 Openness

1. The HMIS Lead Agency will post the Privacy Notice on the HMIS Lead Agency web page and will provide a copy of this document to any individual upon request.
2. Participating Agencies must post a copy of the Privacy Notice at each workstation where HMIS data is gathered or entered.
3. Participating Agencies that serve non- English -speaking clients must also post the appropriate translation of the Privacy Notice that has been approved by the HMIS Lead.
4. Outreach workers must carry a copy of the Privacy Notice (including a copy of the Spanish translation, if applicable) in the field.
5. Participating Agencies must state in the Privacy Notice that the privacy policies may be amended at any time and that amendments may affect information obtained by the Participating Agency before the date of the change.
6. Participating Agencies should include in the Privacy Notice the contact information for its HMIS Representative for purposes of seeking additional information or submitting complaints.
7. Participating Agencies will provide a copy of the *HMIS Privacy Policies Section* in this document to anyone who requests it. The section will also be posted on the HMIS Lead Website.

9.5 Access and Correction Standards

1. Participating Agencies must allow a client to inspect and to have a copy of any PII data elements about the client or their minor household members.
2. Participating Agencies must offer to explain any information that the client may not understand.

3. Participating Agencies must consider any request by a client for correction of inaccurate or incomplete PII pertaining to that client. A Participating Agency is not required to remove any information but may, alternatively, mark information as inaccurate or incomplete and supplement it with additional information such as an indicator of data quality.
4. Participating Agencies must maintain an audit trail of requests for correction of inaccurate or incomplete PII, documenting the name of the requester, the date of request, nature of request, and resulting action.

9.6 Accountability and Privacy Complaints

9.6.1 Privacy Complaints

1. A privacy or confidentiality breach refers to the inappropriate use of client information, unauthorized sharing, or failing to protect data from open view.
2. Participating Agencies are expected to develop and maintain procedures for investigating and responding to Privacy Complaints and share those procedures with the HMIS Lead.
3. Participating Agencies and HMIS Lead Agency will post a notice anywhere HMIS data is collected or accessed that articulates the reporting mechanism for suspected breaches of client confidentiality. The notice will include contact information for the agency's HMIS Representative. The notice will include additional instructions for reporting anonymously.
4. All privacy complaints must be reported to the agency's HMIS Representative within a time frame in accordance with the agency's internal policy. A complaint may be reported directly to the HMIS Lead Agency in writing to hmis@baltimorecity.gov or 7 E. Redwood Street, 5th Floor, 21202.
5. A complaint should trigger HMIS Participating Agency's investigation procedures. A complaint investigation that confirms a breach of confidentiality or unauthorized use of client's information should be reported to the HMIS Lead Agency.
6. Privacy complaints will receive a written response within 30 days.
7. Participating Agencies and HMIS Lead Agency will maintain records of all privacy complaints, responses and outcomes for 7 years from the date of the complaint.

9.6.2 Confidentiality Training and Acknowledgement

1. All users granted HMIS access must first complete HMIS New User Training, which addresses HMIS Confidentiality policies and Procedures.
2. Users must sign an HMIS Confidentiality Acknowledgement Form, as noted in 3.4.4 System User Responsibilities.

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

9.7.1 Victim Service Providers

1. In accordance with the Violence Against Women Act, programs whose primary mission is to serve victims of domestic violence are prohibited from entering personally identifying information about victims into HMIS. Victim service providers receiving HUD funds must use a comparable database that adheres to the same technology data standards as mainstream HMIS systems.
2. Victim service providers must provide aggregate information in reports to HUD. Information in these reports must be non-identifying, which can include aggregate totals or other demographic information that does not identify a victim.

9.7.2 Mainstream Service Providers

1. A mainstream agency that is serving a victim of domestic violence, dating violence, sexual assault, or stalking must explain the potential safety risks for victims and the client's specific options to protect her/his data, such as designating her/his record as hidden/closed to other agencies. The Privacy Notice must clearly state the potential safety risks for domestic violence, dating violence, sexual assault or stalking victims and delineate the information sharing options.
2. All Participating Agency staff collecting client consent must be trained on the protocol for educating victims about their individual information sharing options.

10 Data Quality Plan

Data quality is a term that refers to the degree to which a project satisfies requirements related to data. A data quality plan defines these requirements, assures activities exist to prevent errors and establishes standard procedures to control quality. As a result, a data quality plan can better position the CoC to achieve strategic objectives.

This plan specifies requirements for relevant, measurable attributes utilized to assess data quality: coverage, timeliness, completeness, accuracy and consistency.

10.1 Coverage

Coverage refers to the extent to which an HMIS covers or includes participation from mandated residential and non- residential projects in the CoC geographic area.

1. For lodging, or residential projects, bed coverage is calculated by dividing the number of HMIS participating beds by the total number of year-round beds.
2. For non-lodging, or services-only, projects, service-volume coverage is calculated for each HUD-defined services-only project category, such as street outreach. The service-volume coverage rate is equal to the number of persons served annually by the projects that participate in the HMIS divided by the number of persons served annually by all CoC projects within the HUD-defined category.

While the CoC strives for 100% coverage rates in all categories, the CoC sets forth minimum coverage rates as compliance requirements.

Requirements:

Project Category	Minimum Coverage Rate	Target Coverage Rate
Emergency Shelter	70%	90%
Transitional Housing	90%	100%
Permanent Supportive Housing	90%	100%
Street Outreach	70%	90%

Safe Haven	90%	100%
Rapid Re-housing	90%	100%
Homelessness Prevention	90%	100%
Supportive Services Only	70%	90%

Procedure:

1. For lodging projects, the HMIS Lead will establish a baseline bed coverage rates upon completion of the annual Housing Inventory Count.
2. For non-lodging projects, the HMIS Lead will establish a baseline service-volume coverage as part of the CoC registration process.

10.2 Timeliness

Data entered in a timely manner can reduce human error that occurs when too much time has elapsed between the data collection, or transaction, and the data entry. The individual doing the data entry may be relying on handwritten notes or their own recall of a case management session, a transaction or a project exit date; therefore, less time between data collection and entry increase the odds of higher quality data. Timely entry also ensures that the data is accessible when it is needed, either proactively (e.g. monitoring purposes, increasing awareness, meeting funder requirements), or reactively (e.g. responding to requests for information, responding to inaccurate information).

2. All projects are required to enter Universal Data Elements, Assessments, and Housing Check-ins/Check-Outs within 24 business hours of client contact.

Procedure:

1. The HMIS Lead will assess timeliness by issuing each project a quarterly Data Quality Report Card, which includes a score for data timeliness of new enrollments entered in the previous quarter. This will be based on the HMIS Data Entry Timing report.
2. The HMIS Help Desk has the authority to monitor and address timeliness issues at any time.

10.3 Completeness

Missing data can negatively affect the ability to provide comprehensive care to clients, including eligibility determination

1. All agencies agree, upon HMIS implementation, to adopt and enforce intake and assessment procedures that align with HMIS data collection requirements to prevent incomplete data collection.
2. All projects that use HMIS must enter data on one hundred percent (100%) of clients.
3. While “client doesn’t know” and “client refused to answer” are eligible responses to individual client intake and assessment questions, the CoC defines acceptable rates for these total

"unknown" responses at the project level based on data element and project type considerations.

Standard Average and Upper Limit for Unknown Responses

	SO/Drop-ins (Pre-engagement in Services or case management)	SO/Drop-ins (Pre-engagement in Services or case management)	ES, SH	TH, PSH, SSO, HP, RRH
First & Last Name	10%	0%	0%	0%
Social Security Number	50%	5%	5%	5%
Date of Birth	30%	2%	2%	2%
Race	30%	5%	5%	5%
Ethnicity	30%	5%	5%	5%
Gender	30%	5%	5%	5%
Veteran Status (Adults only)	30%	5%	5%	5%
Disabling Condition (Adults only)	30%	5%	5%	5%
Residence Prior to Project Entry	N/A	0%	0%	0%
Length of Stay	N/A	10%	30%	10%
Length of Time on Street, ES or SH	N/A	10%	30%	10%
Income & Benefits (At project entry)	N/A	2%	30%	2%
Income & Benefits (At project exit)	N/A	10%	50%	10%
Other Program Specific Data Elements	N/A	5%	30%	5%

Destination at Exit	N/A	10%	50%	10%
Bed Check In Date*	N/A	N/A	0%	0%
Bed Check Out Date*	N/A	N/A	0%	0%

Procedure:

1. The HMIS Lead will assess completeness by issuing each project a quarterly Data Quality Report Card, which includes a score for data completeness based on the HUD Data Quality report Section II Overall Completeness rate for PII
2. Data Completeness will be assessed as a part of HMIS Provider Monitoring. When the HMIS Lead finds data completeness fails to satisfy requirements, it will issue a finding and corrective action in the post-monitoring report. In consultation with the HMIS Lead, the agency will implement a plan for corrective action based upon the findings.

10.4 Accuracy

1. All data entered into the CoC's HMIS shall be a reflection of information provided by the client, as documented and update by the data collector with documentation for reference.
2. Intentionally recording inaccurate information is strictly prohibited, except in cases when a client refuses to provide correct personally identifiable information.
3. Agencies will implement appropriate policies and procedures to ensure accurate data collection. This policy may be monitored by the HMIS Lead at any time.
4. Missing or anonymous is only acceptable when a client refuses to provide his or her personally identifiable information, as well as that of dependents, and the project, in accordance with all other requirements, does not prohibit it. In these cases, it is permissible for the agency to enter client data under an alias that will not be made visible or accessible to any other agency.
    a. The agency is responsible for any internal duplication of services as a result of inaccurate data.
    b. If accurate information is later obtained, then the agency should correct the client data in a timely manner; upon correction and provision of client consent to release information, the client data may be shared with agencies in HMIS.

Procedures:

1. HMIS Lead will assess accuracy through HMIS Participating Agency Monitoring visits. The HMIS Lead will compare a random sampling of client paper files to HMIS client files.
2. Monitoring will exclude data on outreach contacts not yet engaged in a project.
3. When the HMIS Lead finds data completeness fails to satisfy requirements, it will issue a finding and corrective action in the post-monitoring report.
4. The agency is responsible for providing any and all documentation for the purposes of the review.
5. In consultation with the HMIS Lead, the agency will implement a plan for corrective action based upon the findings.

10.5 Consistency

Consistency refers to the standard and uniform practice for implementation, data collection and data entry across all projects in the HMIS. Inconsistency hinders an agency's ability to satisfy requirements as they relate to timeliness, completeness and accuracy.

1. All prospective agencies will implement HMIS in consultation with the HMIS Lead, providing access to project assets (e.g. intake and assessment forms, eligibility requirements) and complying with HMIS Lead's recommendations consistent with best practice.
2. The HMIS Lead may delay or cancel implementation if an agency does not faithfully participate in the process.
3. Upon implementation, all HMIS users shall complete training before they may access the system.

Procedure:

1. The HMIS Lead Agency will assess consistency by issuing each project a quarterly Data Quality Report Card, which includes a score for data consistency based on instance of duplicates created by the Agency with an exact match for First Name, Last Name, DOB and SSN.
2. The HMIS Participating Agency may request the names of system users responsible for duplicate record creation.
3. To resolve duplication, the HMIS Lead may request additional information to properly identify clients with incomplete data and rule out any false positives. If duplication persists, the user in question must participate in additional training.

10.6 Compliance, Enforcement and Incentives

1. Compliance with the HMIS Data Quality Plan will be monitored by two primary methods:
    a. Quarterly HMIS Data Quality Report Cards
    b. HMIS Participating Agency Monitoring
2. If the agency repeatedly fails to satisfy data quality requirements and implement corrective action, the HMIS Lead may find the agency in violation of the terms and conditions for HMIS participation which may culminate in loss of project funding for those agencies with HMIS participation requirements.
3. The agency may appeal to the Data and Performance Committee before any loss of funding based on HMIS compliance. Any decision by the committee is final.
4. To incentivize compliance with the plan, the HMIS Lead may choose to publically recognize achievement in the area of data quality.

11 HMIS Data Quality Report Cards

- For the purposes of monitoring adherence to the HMIS Data Quality Plan, gain greater insight into the reliability of HMIS data, as well as to identify projects in need of additional technical assistance, the HMIS Lead will issue Quarterly HMIS Data Quality Report Cards for each project, which will issue a grade for the project's Data Completeness, Data Timeliness and Data Consistency.

- The data quality areas and grade scales were developed with approval from the Data & Performance Committee. Any changes to the Data Quality report cards must be approved by the Data & Performance Committee.

- The HMIS Data Quality Report Cards will be delivered electronically to the HMIS Representative, and/or any additional Participating Agency contacts designated by the HMIS Representative.

- The HMIS Data Quality report cards will be issued quarterly, following the Federal fiscal year (October 1 – September 30) in the month following the close of the quarter (January, April, July, October).

- Data for the report cards will be compiled three business days after the close of the quarter, during which time projects may make data corrections to improve their data quality score.

- Projects with a grade of C or lower within any individual data quality error over three consecutive report cards will be contacted for additional staff training or technical assistance within the data quality area. The HMIS Lead will monitor the project for improvement after interventions. If the project fails to improve, the HMIS Lead will create an action plan with the HMIS Participating Agency to continue to attempt to resolve the issue.

- The HMIS Lead reserves the right to make exceptions to Data Quality Report Card issuance or to modify Data Quality Report Card scoring if circumstances should dictate (one example would be if there is a delay in a project's onboarding to HMIS resulting in the need to perform back-data entry, the HMIS Lead may decide not to issue a timeliness score for that quarter).

11.1 Data Completeness Scoring

1. Data Completeness will be scored based on the Overall error rate % for PII in section 2 of the HUD Data Quality Report for each project for the previous quarter.
2. Completeness grades will be issued on the following scale:

Completeness - Overall error rate % by project type					
	A	B	C	D	F
Street Outreach	0 - 5%	5 - 10%	10 -15%	15 - 25%	25% or higher
Day Shelter	0 - 5%	5 - 10%	10 -15%	15 - 25%	25% or higher
Emergency Shelter (NbN)	0 - 5%	5 - 10%	10 -15%	15 - 25%	25% or higher
Emergency Shelter (Entry/Exit)	0 - 3%	3 - 5%	5 -10%	10-15%	15% or higher
Homelessness Prevention	0 - 3%	3 - 5%	5 -10%	10-15%	15% or higher
Supportive Services Only	0 - 1%	1 - 3%	3 - 5%	5 - 10%	10% or higher
Safe Haven	0 - 1%	1 - 3%	3 - 5%	5 - 10%	10% or higher
Transitional Housing	0 - 1%	1 - 3%	3 - 5%	5 - 10%	10% or higher
Rapid Re-Housing	0 - 1%	1 - 3%	3 - 5%	5 - 10%	10% or higher
Permanent Supportive Housing	0 - 1%	1 - 3%	3 - 5%	5 - 10%	10% or higher

11.2 Data Consistency Scoring

1. Data Consistency will be scored based on duplicate merges performed by the HMIS Lead agency where the duplicate record has an exact match for First Name, Last Name, Date of Birth and Social Security Number. The agency that created the most recent record will be marked as creating the duplicate.
2. Because duplicates can only be tracked on an agency-wide basis, the Consistency score will apply to all projects within an agency.

3. The HMIS Lead will track the HMIS user that created the duplicate so training needs can be targeted.
4. Consistency grades will be issued on the following scale:

Consistency - Number of duplicates created by agency					
	A	**B**	**C**	**D**	**F**
All projects	0 duplicates	1 - 2 duplicates	3-4 duplicates	5 - 6 duplicates	7 + duplicates

11.3 Data Timeliness scoring

1. Data Timeliness will be scored based on the time elapsed between the client's Project Start Date and the Creation Date of new client enrollments created in the previous quarter. This will be reported with the HMIS Data Entry Timing report.
2. If no new enrollments were created in the previous quarter, the timeliness score will be omitted from the project's report card and GPA calculation.
3. Timeliness grades will be issued on the following scale:

Data Timeliness - Time elapsed since client contact to data entry					
	A	**B**	**C**	**D**	**F**
All projects	0 - 2 days	3 - 5 days	6 - 8 days	8 - 10 days	11 + days

11.4 Overall project grade

1. An overall project grade will be calculated by averaging together the grades from each data quality area.

12 HMIS Participating Agency Monitoring

HMIS monitoring is completed to ensure that projects are adhering to the Baltimore City HMIS policies and procedures in their work with HMIS data, particularly security and privacy protocols and minimum data requirements. All participating agencies are subject to HMIS monitoring once annually, completed either as a part of their CoC or State DHR monitoring processes, or via a unique HMIS site-visit.

HMIS monitoring supplements monthly data quality reporting provided to participating agencies in accordance with the Baltimore City HMIS data quality plan.

Due to the COVID -19 pandemic, all on-site monitoring visits were suspended. On November 18, 2020 the Data and Performance Committee has agreed to further postpone HMIS on-site monitoring and any revisions to the policy at this time. The committee has agreed to revisit the on-site monitoring Agency Monitoring Policy in the Spring 2021.

The Committee has agreed that remote monitoring will be performed via the data quality reviews of the Longitudinal System Analysis Report, Housing Inventory Count, Quarterly Data Quality Report Cards, and the System Performance Measure Reports.

The suspension of on-site monitoring will remain in effect until deemed safe to resume by

Monitoring plans and schedules have been adjusted accordingly to accommodate the temporary suspension of on-site monitoring.

Monitoring rates & frequency

1. 100% of HMIS participating agencies will be monitored on site during the introductory phase of the HMIS Monitoring Process, expected to last through FY19. After the introductory phase, the HMIS Lead will develop an HMIS Monitoring Risk Assessment to determine project monitoring.
2. Monitoring will occur for specific projects.
3. Agencies with multiple projects must have all projects monitored at least once in a three year period to ensure oversight of all data collection sites.
4. Participating agencies with multiple projects that operate from the same location may be monitored in one visit. Participating agencies with multiple projects that operate from separate locations may require multiple visits to complete monitoring.
5. HMIS monitoring may be completed via a regularly scheduled program-monitoring visit occurring as a part of funding-based monitoring (CoC or state funding). Projects that do not get captured in these monitoring visits will have HMIS-specific monitoring visits scheduled.

Monitoring Procedures:

1. HMIS Reps will be notified at least four weeks in advance of their monitoring date. Projects may request rescheduling of their monitoring visit with the availability of HMIS staff.
2. The length of site visits will depend on the size and type of project. Most monitoring visits will take a day or less.
3. All sites where HMIS data is processed should be monitored. (If data is processed in the field, such as during outreach or home visits, devices used during field data collection will be monitored).
4. HMIS Representatives will receive an HMIS Data Quality Monitoring self-assessment which must be completed ahead of the site visit provided upon arrival of the HMIS Monitor.
5. The HMIS Monitor will utilize the Baltimore City HMIS Monitoring Checklist to guide the monitoring visit.
6. The sample size of paper files and workstations monitored will be determined based on the number of clients enrolled and the number of end users supporting the project.
7. A post-monitoring report will be issued within 30 days following the site visit. The post-monitoring report will include findings and any corrective actions, including steps that must be taken to resolve the issues.
8. Corrective actions must be completed within 30 days of report issuance.
9. The appropriate Program Compliance staff will be notified if an agency is found out of compliance with funding requirements.
10. The HMIS Lead may conduct a follow up visit to verify completion of corrective actions.
11. Failure to complete corrective actions may result in revocation of HMIS access until such time the corrective actions are implemented.