*Cleveland/Cuyahoga County Continuum of Care*

# *Homeless Management Information System*

# *Policies & Procedures Manual*

*Office of Homeless Services*
*310 W. Lakeside Ave, Suite 595*
*Cleveland, Ohio 44113*
*Phone: (216) 420-6744*
*Ohio Relay Service (TTY): 1-800-750-0750*
*Fax: (216) 698-6604*

*Cleveland/Cuyahoga County Continuum of Care*
*Homeless Management Information System*

## Overview:

In 2001, Congress established a national goal and directive for HUD that all communities receiving HUD homeless program funding collect an array of data, including unduplicated counts of homeless, the use of services and the effectiveness of local assistance systems. In order to achieve this objective, HUD mandated that all communities develop a Homeless Management Information System (HMIS).

Beginning with the 2003 Continuum of Care (CoC) and Emergency Shelter Grants (ESG), the U.S. Department of Housing and Urban Development (HUD) required all grantees and sub-grantees to participate in their local HMIS. This policy is consistent with the Congressional Direction for communities to provide data to HUD on the extent and nature of homelessness and the effectiveness of its service delivery system in preventing and ending homelessness.

**Mandated Participation**

Projects authorized under HUD's McKinney-Vento Act, as amended by the HEARTH Act, and mandated by Federal, State, or Local funding sources must meet the minimum participation standards as outlined in this Policies and Procedures Manual.

**Voluntary Participation**

The Cleveland/Cuyahoga County Continuum of Care (CoC) strongly encourages homeless service providers to participate in the local HMIS. The HMIS lead agency works regularly with non-funded providers to communicate the benefits of HMIS and encourage participation.

The HMIS and its operating policies and procedures are structured to comply with the most recent https://files.hudexchange.info/resources/documents/FY-2022-HMIS-Data-Standards-Manual.pdf

## What is a Homeless Management Information System?

A Homeless Management Information System (HMIS) is a locally administered electronic data collection tool designed to capture client-level information over time on the characteristics, service needs, and service utilization of men, women, and children experiencing homelessness.

The HMIS Lead Agency, Cleveland/Cuyahoga County Office of Homeless Services (OHS), holds the contract with Bitfocus Inc. for the use of an HMIS application known as *Clarity*. Under this agreement, OHS is the licensed administrator of *Clarity* which is managed by the System Administrator. The HMIS System Administrator ensures that the system is available to agency partners and providers within the Cleveland/Cuyahoga County Continuum of Care.

## HMIS Solution:

Cuyahoga County has adopted the use of *Clarity* (from Bitfocus Inc.) as its HMIS software solution. *Clarity* is a web-based application that requires no local software installation. It provides automatic reports to meet HUD reporting requirements and offers flexibility so that local agencies can customize its use for local needs. This platform was selected by a group of representatives of the Local Continuum of Care in 2020, following a highly participatory process of analysis of system needs and comparative examination of several top-rated software platforms.

The Homeless Management Information System (HMIS) project is administered by the Cleveland/Cuyahoga County Office of Homeless Services. The project utilizes the Internet-based technology to assist homeless service organizations across Cuyahoga County to capture information about the clients that they serve.

**Potential benefits for agency and Program managers:**
When aggregated, information can be used to garner a more complete understanding of clients' needs and outcomes, and then used to advocate for additional resources, complete grant applications, conduct evaluations of project services, and report to funders such as HUD. The software has the capability to generate the revised HUD Annual Progress Report (APR).

**Potential benefits for homeless men, women, and children and case managers:**
Directors, program managers, employees, and case managers can use the software as they assess their clients' needs to inform clients about services offered on site or available through referral. Employees and clients can use on-line resource information to learn about resources that help clients find and keep permanent housing or meet other goals clients have for themselves. Service coordination has been improved with the implementation of Coordinated Intake and Assessment and the sharing of information among HMIS Participating Agencies (with written consent) who are serving the same clients.

**Potential benefits for community-wide Continuums of Care and policy makers:**
Involvement in HMIS provides the capacity to projects within a Continuum to generate automated HUD APRs and to utilize the aggregate data to inform policy decisions aimed at preventing and reducing the number of persons experiencing homelessness at the county level.

**Vision for HMIS**
HMIS within the Cleveland/Cuyahoga County Continuum of Care continues to develop. The goals of our HMIS system demonstrate our united effort and dedication towards providing targeted services in order to reduce the number of newly homeless, reduce the length of stay for those who are homeless and reduce the number returning to shelter. We strive to provide the following:

- Coordinated case management across agencies, programs, projects and services
- Comprehensive information on clients served through a shared system of client records
- Integration of HUD's requirements for a Coordinated Entry (CE) system, referred to locally in Cleveland/Cuyahoga County as ***Coordinated Intake***
- Coordinated bed management
- An effective tool for tracking referrals and outcomes consistent with local planning and the Federal Plan to End Homelessness
- Customized assessments and reports which allow us to
    - Identify needs, resources and gaps through the use of data
    - Enhance strategic planning efforts
    - Continue to Inform public policy regarding the nature and extent of homelessness in Cuyahoga County
    - Work with other local/state/federal entities to conduct cross-system analysis

This document provides the policies, procedures, guidelines, and standards that govern operations, as well as roles and responsibilities for OHS Staff and Participating Agency staff.

## Terms and Definitions

**System Administrator** – The person with primary responsibility for managing the HMIS. The System Administrator provides technical database administration support to ensure HMIS data are well organized, accurate, complete, accessible for reporting and client case planning, and HMIS system users comply with standards for HMIS privacy, security, and data quality.

**Participating Agency** – An agency contributing data to the HMIS. Participating agencies must comply with standards for HMIS participation including system security, client privacy, and data quality.

**End User** – a person associated with a Participating Agency and authorized by the System Administrator to access the HMIS. End Users may have different levels of HMIS access that may include view only access, ability to enter new data, ability to enter new data and edit previously contributed data, and ability to generate reports from HMIS data.

**Cleveland/Cuyahoga CoC Advisory Board** – the primary governing body for the Cleveland/Cuyahoga Continuum of Care. As the CoC governing entity, the CoC Advisory Board establishes operating policies and guidelines for all CoC operations, including HMIS.

**Lead Agency** – The HMIS Lead Agency is authorized by the Cleveland/Cuyahoga CoC Advisory Board to manage the HMIS project. Management responsibilities including holding the contract with the HMIS software vendor and any other vendors supporting the HMIS project. The Lead Agency ensures the HMIS project and all associated HMIS activities are carried out in compliance with HUD's HMIS Data and Technical Standards.

**Data Committee** – A subcommittee of the Cleveland/Cuyahoga CoC Advisory Board with responsibility for oversight of the HMIS Lead Agency and all HMIS supporting documentation, including HMIS policies and procedures, privacy policy, consent protocols, data security protocols, data quality protocols, and HMIS quality assurance efforts.

**Agency Administrator** – The person at a Participating Agency who serves as the primary contact between the Participating Agency and the HMIS Lead Agency. Agency Administrators provide additional technical support and HMIS system coordination for staff of the Participating Agency.

**Security Officer** – the person at the Lead Agency and/or Participating Agency responsible for ensuring compliance with the HUD HMIS security standards and any additional security protections identified in the HMIS Policies and Procedures.

**Participation Agreement** – An agreement between the Lead Agency, on behalf of the Cleveland/Cuyahoga CoC, and a Participating Agency. The Participation Agreement

## Governing Principles

**Access to HMIS**

Each agency will designate specific staff as HMIS End Users. Each User will be issued one personal user license: **login ID** and **password** for access to the database. Each agency will also determine the user access level for each of its licensed Users. Licenses and access to the database will be cancelled immediately for any User that terminates employment. The Agency Administrator, Program Manager, or Director at each Participating Agency **will inform the**

**System Administrator of staff changes** within one business day of a staff member leaving the agency

- Clients have the right to see their information in HMIS. If a client requests to see their information, the Participating Agency/User who receives the request must review the information with the client.

**Persons to Enter into HMIS**
Adults and children who are homeless, as defined by the Department of Housing and Urban Development, will be entered into HMIS with informed/written consent.

**Data Entry and Data Sharing**
Participating Agencies must collect the required set of data elements for each client. As outlined in the latest version of the HUD Data Standards, this includes the Universal and Program Specific Data Elements. In addition, Participating Agencies are required to review and update any/all data elements for each client served at the time of project entry, annual review and at exit.

Participating Agencies understand that only the individual who created the assessment screen (Coordinated Intake), or an authorized person by originating agency, has the ability to edit information within the assessment screen. Each Participating Agency will be responsible for completing a separate assessment, as needed, in order to accurately reflect changes to data for those clients served by the agency itself.

**Protected Information**
In the HMIS Record, there are certain services, referrals, and agencies not to be shared with other agencies.

1. Domestic Violence
2. HIV/Aids

**Shared Information**
Each Participating Agency must complete and comply with the Agency Partnership Agreement.

Each individual HMIS user must complete and comply with the User Code of Ethics, Policy, and Responsibility Statements.

Each Participating Agency will have access to view all open client records and direct access to data entered by its own staff about the clients they serve. Written consent must be given by clients in order for their identifying information to be entered into HMIS and shared among agencies.

- Each Participating Agency must conduct periodic reviews to ensure appropriate written documentation (Client Release of Information) indicating client consent of data entered into HMIS.
- Identifying client information will only be shared among agencies that have signed the Agency Partnership Agreement (CoC Memorandum of Understanding). At any time, the client has the right to see a current list of CoC participating agencies.
- Additional agencies may join with notification and consent of the CoC Lead Agency.
- HMIS Users will maintain HMIS data in such a way as to protect against revealing the identity of clients to unauthorized agencies, individuals, or entities.

- No information will be entered for clients currently fleeing or in danger from a domestic violence situation and being served by a Victim Service Provider.
- Clients may choose to no longer participate in HMIS at any time but must notify the Participating Agency via a signed "Consent to Rescind Participation in HMIS" form. This form must be submitted to the HMIS System Administrator.
- Clients may not be denied services based on their choice to withhold their consent.
- Participating agencies must maintain a comprehensive record (hard copy or electronic) for each client refusing/rescinding authorization to participate in HMIS.
- De-identified data may be used for the purposes of evaluation and research.

**Children's Data:** Information about clients who are under the age of 18 is always restricted. It is the User's responsibility to designate the information as "private". Children's data may be shared if a parent or guardian lists the child on a signed "Release of Information Authorization" form.

**Data Integrity:** Data is the most valuable asset of the HMIS Project. It is our policy to protect this asset from accident or intentional unauthorized modification, disclosure or destruction.

**Access to Client Records**

The Client Records Access policy is designed to protect against the recording of information in unauthorized locations or systems. Only staff that work directly with clients or who have administrative responsibilities will receive authorization to look at, enter, or edit client records. Additional privacy protection policies include:

- Client has the right to not answer any question, unless entry into a service project requires it.
- Client has the right to know who has added to, deleted, or edited their client record.
- Client information transferred from one authorized location to another over the web is transmitted through a secure, encrypted connection.
- Client information is stored in an encrypted database.

**Quality Assurance**

Participating Agencies are responsible for timely, accurate and complete entry of client-level data.

- Central Intake (CI) is responsible for obtaining and entering the initial, complete data set for most individuals or family members served. CI will also enter all appropriate client referrals to CoC Participating Agencies.
- The Participating Agency, receiving referrals, will review and enter information in HMIS about individuals participating in an agency project.
- The Participating Agency will not enter fictitious or misleading data on an individual or household. Nor will the agency enter data that misrepresents the number of clients served or beds provided.
- Each Participating Agency will strive for real-time, or close to real-time, data entry. This is defined by either immediate data entry upon the client receiving an assessment or within one business day of the client assessment.
- Each Participating Agency must maintain a current copy of the Client Release of Information on file for each individual or family member served.

- The Participating Agency is responsible for each project's data quality within the respective provider tree and the percentage of "null/missing" and "unknown/don't know/refused" values relative to HUD required elements.

***See Data Quality Plan***

**End User Ethics**
Any deliberate action that adversely affects the resources of any participating organization, institution, employee, or individual is prohibited. Users should not use the HMIS computing resources for personal purposes. Users must not attempt to gain physical or logical access to data or systems for which they are not authorized.

**Computer Crime**
Computer crimes violate State and Federal law as well as the Cleveland/Cuyahoga County HMIS security Policy and Procedures. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, data, or printouts; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under State and Federal law, held civilly liable for their actions, or both.

**Application Software**
Only tested and controlled software should be installed on networked systems. Use of unevaluated and untested software outside an application development environment is prohibited.

**Technical Support**
The System Administrator will be responsible for the training of all Participants in the use of the HMIS program. Cuyahoga County Information Services Center will maintain the server. Each Participating Agency is responsible for providing and maintaining computer hardware and Internet Service.

**HMIS End User Training**
Prior to use, all users are required to attend training sessions. All Agency Administrators are required to attend 2 days of Agency Administrator training. Agency Administrators will be responsible for training their staff. The HMIS System Administrator will provide trainings for all HMIS End Users on an as needed basis.

## ROLES AND RESPONSIBILITIES

### Cleveland/Cuyahoga CoC Advisory Board

The CoC Advisory Board serves as the primary governing entity for the Cleveland/Cuyahoga Continuum of Care. As the CoC governing entity, the CoC Advisory Board establishes operating policies and guidelines for all CoC operations, including HMIS.

The Cleveland/Cuyahoga CoC Advisory Board HMIS-related responsibilities.

i) The CoC Advisory Board designates the HMIS Lead. The Cuyahoga County Office of Homeless Services (OHS) is the current Homeless Management Information System (HMIS) Lead, until and unless the Advisory Board designates another HMIS lead agency.
ii) The CoC Advisory Board must ensure that the HMIS Lead agency is operating in compliance with current HUD HMIS regulations and other applicable laws. The Advisory Board and HMIS Lead agree to update HMIS operational documents and HMIS policies and procedures to comply with any updates to HMIS standards established in notices or other guidance, within the HUD- specified timeframe for such changes.
iii) Every five years the CoC Advisory Board reviews annual evaluations and any corresponding corrective actions. Upon conducting this review if any areas of concerns are found to be not addressed, the CoC Advisory Board will vote on whether the HMIS Lead agency is compliant with pertinent regulations and CoC Board expectations. Additionally, the CoC Advisory Board shall consider if the HMIS lead has taken appropriate corrective actions to improve any areas of concerns.
    a. The timeline for the five-year review will begin upon approval of the HMIS Evaluation Plan by the HMIS Data Committee and the CoC Board and is expected to begin in 2021.
iv) If the CoC Advisory Board finds that the HMIS Lead has not taken acceptable measures to improve on areas of concern outlined by the HMIS Data Committee, the CoC Advisory Board may vote to develop a timeline for corrective actions or vote to assign a new HMIS Lead Agency.
v) If the CoC Advisory Board votes to assign a new HMIS Lead, the Board shall direct the Lead Agency and the HMIS Data Committee to conduct a Request For Interested (RFI) parties and corresponding Request For Qualifications (RFQ) process to solicit and select a HMIS Lead.
    a. In partnership with the HMIS Data Committee, this RFI/RFQ process will be conducted by CoC Lead Agency.
    b. Upon receiving and reviewing received qualification proposals, the Lead Agency and the HMIS Data Committee shall make recommendations for the CoC Board for a final vote to select the new HMIS Lead.

### HMIS Lead Agency

The HMIS Lead Agency, Cleveland/Cuyahoga County Office of Homeless Services (OHS), holds the contract with Bitfocus, Inc. for the use of Clarity. Under this agreement, OHS is the licensed administrator of Clarity which is managed by the System Administrator.

As the HMIS Lead Agency, the OHS ensures that all HMIS activities are carried out in accordance with the HEARTH Act of 2009 and the relevant HMIS Data Standards.

The HMIS Lead Agency must develop new HMIS policies and procedures annually to remain in compliance with changes in Coordinated Intake, HMIS Data Standards, and any new regulations. Additionally, the HMIS Lead Agency must review and update existing Documents including the Privacy Plan, Data Quality Plan, Security Plan, Governance Charter & Policies and Procedures at least annually, ensuring compliance with any new federal, state, or local regulations. While the final operational responsibility resides with the HMIS Lead Agency, OHS divides accountability among 3 parties:

1. **HMIS Lead Agency**. Responsible for updates to the HMIS Policies and Procedures and the creation of or any revisions to existing documents for HMIS in compliance with new regulations and system changes. The HMIS Lead agency houses the HMIS System Administrator responsible for all aspects and oversight of the HMIS.
2. **HMIS Data Committee**. Responsible for reviewing, providing feedback and approving any HMIS procedural and/or document changes.
3. **CoC Advisory Board**. Responsible for final approval of annual revisions to the HMIS Policies and Procedures.

**The HMIS System Administrator is responsible for:**

- Providing training support to Participating Agencies by determining training needs of end users, developing training materials and conducting training sessions;
- Serving as the primary liaison with the HMIS vendor to advocate and resolve issues;
- Providing technical support by troubleshooting data with Participating Agencies;
- Managing user accounts and access;
- Managing system enhancements/updates and modifications;
- Fulfilling and assisting with reporting requirements for the CoC;
- Developing regular reports based on local CoC goals and objectives;
- Providing oversight of HUD/CoC quality and security standards;
- Working with CoC committees to coordinate the HMIS effort;
- Monitor participating agency use of HMIS for compliance with HMIS Policies and Procedures, Privacy Plan, Security Plan and HMIS Data Quality Plan, and HMIS Data Standards.

**HMIS Participating Agencies**

Any agency who participates in HMIS must complete an Agency Memorandum of Understanding and agree to abide by the policies and procedures outlined in this manual. Participating agencies are responsible for their client level data; furthermore, each agency is responsible for the integrity and security of their agency's client data.

Participating agencies are responsible for their agency end users and ensuring that they comply with the policies and procedures manual.

**Each Participating Agency must designate an Agency Administrator and a backup Agency Administrator responsible for:**

- Serving as the primary contact between their agency's end users and the HMIS System Administrator;

- Reporting any changes regarding HMIS Provider Profile Information to the HMIS System Administrator;
- Providing technical support by troubleshooting data and escalating unresolved issues to the HMIS System Administrator;
- Notifying all of their agency end users of system updates, changes or other relevant information;
- Notifying HMIS System Administrator of personnel changes as it relates to HMIS;
- Conducting new and refresher trainings to agency end users;
- Assuring only trained, designated and licensed staff enter and maintain data;
- Monitoring compliance as outlined in the HUD Data Standards;
- Performing routine quality assurance procedures to monitor data quality and promptly make corrections. Develop and provide Agency Internal Data Quality Plan for HMIS;
- Ensuring their agency's adherence to the HMIS Policies and Procedures. Reporting any violations;
- Providing and maintaining computer hardware, software and Internet Service;
- Serving as the HMIS Security Officer for the agency.

*Note: Certain circumstances (sick leave, FMLA, extended vacation, etc.) will require the transfer of an agency's HMIS license from one staff person to another. The existing HMIS Agency Administrator or Executive Director must submit any/all license transfer requests directly to the HMIS System Administrator via email.*

**HMIS Security Officer Responsibilities**

Each HMIS Lead Agency and Participating Agency must designate an HMIS Security Officer. For Participating Agencies, this is the Agency Administrator. This individual is responsible for ensuring compliance with the HUD security standards outlined in the Policies and Procedures described in this document.

**End Users**

End Users are designated by their agency's Executive Director and HMIS Agency Administrator. End Users must sign an HMIS End User Agreement and complete training in order to access HMIS. End Users are responsible for collecting/reviewing/entering all of the HUD-required or other funder-required data elements for each individual and household member, ensuring that data entry complies with the timeliness standards, ensuring that they protect privacy and client confidentiality and for following all other policies and procedures in this manual.

**HMIS Data Committee**

The HMIS Data Committee will be responsible for making recommendations to the CoC Advisory Board. The HMIS Lead Agency will identify and recruit members from HMIS Participating Agencies based on specific criteria and experience in the system. The purpose of this committee is to advise, support and encourage the Cleveland/Cuyahoga County Continuum of Care HMIS operations in the following areas: consumer involvement, quality assurance, planning and accountability.

- Planning, decision-making, evaluation and facilitation for the implementation of HMIS
- Coordination and recommendations to assist projects with participation (i.e. resources, workflow, etc)

- Determining and making recommendations on policies and procedures for the HMIS system
- Evaluating potential projects regarding research efforts and linking HMIS with other databases
- Supporting the rights and privacy of homeless persons as it relates to HMIS.

**HMIS User Group**

The User Group will hold meetings on an adhoc basis for the purpose of addressing implementation and on-going operational issues. The User Group exists for the purpose of information sharing, problem solving, and generating recommendations for the continued improvement of the local project. The User Group will consist of all end users from each of the Participating Agencies and the System Administrator.

## Policies and Procedures

**Title:** **Participation Requirements - Workstation**

**Policy:** All recipients of HUD McKinney-Vento Act funds are required to participate in HMIS. Funded projects include all Continuum of Care, ESG, SHP, S+C and Section 8 moderate Rehabilitation for SRO.

**Purpose:** To provide the structure of on-site support and compliance expectations.

**Scope:** System wide

---

**Workstation Minimum Requirements**

- Intel-compatible 2GHz+ processor.
- Minimum of 40 GB Hard Drive.
- Minimum of 2GB RAM.
- LAN or always-on High Speed Internet Connection (Cable, DSL, Fiber-Optic).
- Recent version of Internet Explorer, Google Chrome, or Mozilla Firefox with proper browser settings for use with SSL based websites.
- Virus protection updates.

**Internet Browser Comparisons**

- Internet Explorer 8 is much faster than Internet Explorer 7.
- Each new release of Firefox tends to be incrementally faster than the previous.
- Most Firefox versions are faster than any Internet Explorer version.
- Safari tends to fall between Firefox and Chrome.
- Chrome has been maintaining its lead as fastest of all.

**System Minimum Requirements**

- **Identification of Site Agency Administrator:** Designation of **one** key staff person and a backup staff person to serve as both the **Agency Administrator and Security Officer** for the site. This person will be responsible for password resets, monitoring application access and maintaining all aspects of security. This person will also be responsible for training new staff persons.
- **Training**: All Agency Administrators will attend required training(s)with the HMIS System Administrator at the Office of Homeless Services. The Agency Administrator is responsible for training all other agency end users.

**Note: Users will NOT be allowed to access the system until ALL Information Security paperwork is complete and signed by Executive Director (or designee).**

- **Interview Protocols:** Agencies must collect all required data elements and any additional data elements established by Federal, State, and Local funders. These data

elements will be available in an Interview Protocol format for use with clients during the initial/assessment process at Coordinated Intake.

- **Participation Agreement:** Agencies are required to sign an Agency Participation Agreement/Memorandum of Understanding stating their commitment to achieve effective use of the system and proper collaboration within the Cleveland/Cuyahoga County Continuum of Care.

**Title:** **Participating Agency Executive Director/Program Manager**

**Policy:** The Executive Director and Program Manager of each participating Agency will be responsible for oversight of all agency staff who generate or have access to client-level data stored in the system software to ensure adherence to the HMIS policies and procedures outlined in this document.

**Purpose:** To outline the role of the agency Executive Director/Program Manager with respect to oversight of agency personnel in the protection of client data within the system software application.

**Scope:** Executive Director/Program Manager in each Participating Agency

---

**Responsibilities**

The Participating Agency's Executive Director and Program Manager are responsible for all activity associated with agency staff access and use of the HMIS data system. They are responsible for establishing and monitoring agency procedures that meet the criteria for access to the HMIS system, as detailed in the policies and procedures outlined in this document.

The Executive Director/Program Manager will be held responsible for any misuse of the system by his/her designated staff. The Executive Director and Program Manager agree to only allow access to the HMIS software system based upon need. Need exists only for those shelter staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.

The Executive Director and Program Manager oversee the implementation of data security policies, standards, and will:

- Assume responsibilities for integrity and protection of client-level, project-level and agency-level data entered into the HMIS system.
- Establish business controls and practice to ensure organizational adherence to the HMIS Policies and Procedures.
- Communicate control and protection requirements to agency custodians and users.
- Authorize data access to agency and assign responsibility for custody of the data.
- Monitor compliance via the agency's Data Quality Plan and conduct periodic reviews.

**Title:** **Participating Agency Administrator**

**Policy:** Participating Agency must designate one person to be the Agency Administrator.

**Purpose:** To outline the role of the site Agency Administrator

**Scope:** Participating Agencies Agency Administrator

---

**Responsibilities**

The Participating Agency agrees to appoint one person and one back up person as the Agency Administrator. This person will be responsible for:

- Serving as the primary contact between their agency's end users and the HMIS System Administrator
- Reporting any changes regarding HMIS Provider Profile Information to the HMIS System Administrator
- Providing technical support by troubleshooting data and escalating unresolved issues to the HMIS System Administrator
- Notifying all of their agency end users of system updates, changes or other relevant information
- Notifying HMIS System Administrator of personnel changes as it relates to HMIS;
- Conducting new and refresher trainings to agency end users
- Assuring only trained, designated and licensed staff enter and maintain data.
- Monitoring compliance as outlined in the HUD Data Standards
- Performing routine Quality Assurance procedures to monitor data quality and promptly make corrections. Develop and provide Agency Internal Data Quality Plan for HMIS
- Ensuring their agency's adherence to the HMIS Policies and Procedures. Reporting any violations
- Providing and maintaining computer hardware, software and Internet Service
- Serving as the HMIS Security Officer for the agency
- Ensuring that access to the HMIS system be granted to authorized staff members only after they have received training and satisfactorily demonstrated proficiency in use of the software and understanding of the Policies and Procedures and agency policies referred to above

The Agency Administrator will also serve as the site HMIS Security Officer and is responsible for the implementation of data security policy and standards, including:

- Administering agency-specific business and data protection controls
- Administering and monitoring access control
- Providing assistance in the backup and recovery of data

**Title:** **User Role**

**Policy:** Users must have specific authorization to access the application.

**Purpose:** To outline the role and responsibilities of the system user

**Scope:** System wide

---

**Responsibilities**

The Participating Agency agrees to authorize use of the HMIS system only to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

Users are any persons who use the HMIS software for data processing services. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure. Users are responsible for protecting institutional information to which they have access and for reporting security violations.

Users must comply with the data security policy and procedures as described in these Policies and Procedures. They are accountable for their actions and for any actions undertaken with their usernames and passwords.

**Title:** **Maintenance of System Operation**

**Policy:** Participating Agencies must meet the technical standards for minimum computer equipment configuration, Internet Connectivity, data storage, and data maintenance program.

**Purpose:** Participating Agencies commit to a reasonable program of data and equipment maintenance in order to sustain an efficient level of system operation.

**Scope:** Participating Agencies

---

**Responsibilities**

The Executive Director or designee will be responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the HMIS Program including the following:

**Computer Equipment**

The Participating Agency is responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization in the HMIS Project.

**Backup**

The Participating Agency is responsible for supporting a backup procedure for any agency system that serves as a source of information for the HMIS.

**Internet Connection**

OHS staff members are not responsible for troubleshooting problems with Internet Connections.

**Data Storage**

The Participating Agency agrees to only download and store data from the HMIS in a secure format.

**Data Disposal**

The Participating Agency agrees to dispose of documents that contain identifiable client level data by shredding paper records, deleting any information from CD-ROM before disposal, and deleting any copies of client level data from the hard drive of any machine before transfer or disposal of property. OHS staff is available to consult on appropriate processes for disposal of electronic client level data.

**Title:** **Implementation of Interagency Sharing Standards**

**Policy:** As part of the implementation strategy of the system software, a Participating Agency must have a client authorization & consent procedures and completed forms in place for electronic data sharing.

Participating Agencies are required to develop procedures for providing oral explanations to clients about the usage of a computerized Homeless Management Information System. Participating Agencies are required to obtain informed consent prior to entering client data into HMIS.

**Purpose:** To indicate the type of client authorization procedures that Participating Agencies must implement for data sharing implementation.

**Scope:** System wide

---

**Informed Consent:** Oral Explanation: All clients will be provided an oral explanation both at the time of Coordinated Intake & Assessment and project entry. Clients will be informed that their information will be entered into a computerized record keeping system. Each Participating Agency will provide an oral explanation of the HMIS project and the terms of consent. The agency is responsible for ensuring that this procedure takes place prior to every client interview. The document Informed Consent must includethe following information:

- **What HMIS is?**
  - Internet based information system that Cleveland/Cuyahoga County Homeless Service Agencies use to aggregate information about the persons they serve.
- **Why the agency uses it**
  - To issue referrals and coordinate service delivery
  - To understand client needs & outcomes
  - To help identify and plan for appropriate resources for persons served
  - To inform public policy in an attempt to end homelessness
- **Security**
  - Only staff that have an HMIS license or who have administrative responsibilities can look at, enter, or edit client records
- **Privacy Protection**
  - No information will be released to a non-participating agency. Information will only be shared with written consent.
  - Client has the right to not answer any question, unless entry into a project requires it
  - Upon written request, the client has the right to view their HMIS record
  - Information that is transferred over the Internet is through a secure connection & is encrypted

- **Benefits for Clients**
  - Case manager tells client what services are offered on site or by referral through the assessment process.
  - Case Manager and client can use information to assist clients in obtaining resources that will help them find and keep permanent housing.

- **Information Release:**
  The Participating Agency agrees not to release client identifiable information to any other non-participating organization pursuant to federal and state law without Informed consent.

- **Federal/State Confidentiality Regulations:**
  The Participating Agency will uphold Federal and State Confidentiality regulations to protect client records and privacy. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations.

  1. The Participating Agency will abide specifically by the Federal confidentiality rules as contained in **42 CFR Part 2** regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal rules prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Participating Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.

  2. If the records released include information of an HIV-related diagnosis or test results, the following statement applies:

     This information has been disclosed to you from confidential records protected from disclosure by state law. You shall make no further disclosure of this information without the specific, written and informed release of the individual to whom it pertains, or as otherwise permitted by state law. A general authorization for the release of medical or other information is NOT sufficient for the purpose of the release of HIV test results or diagnosis.

- **Unnecessary Solicitation:** The Participating Agency will not solicit or input information from clients unless it is essential to provide services, or conduct evaluation or research.

**Title:** **Data Elements Requirements**

**Policy:** All Participating Agencies agree to enter/review/update the standard set of data elements on all clients served within each project.

**Purpose:** To uphold a standard level of coverage

**Scope:** System wide

---

**Responsibilities**

- Data Collection Commitment – All HMIS Data Standard required elements and CoC required elements.

- Commitment to Utilization of Interview Protocol

- Required Data Elements: The Participating Agency is responsible for ensuring that all clients are asked a standard set of questions for use in aggregate analysis. These questions are available in an Interview Protocol format and will initially be provided through Coordinated Intake and Assessment. The Participating Agency agrees to enter, review and update this level of client information into the HMIS software system at the time of project entry, annual review or recertification and project exit.

**Data to be collected by all HMIS Participating Agencies are those essential to the administration of local homeless assistance projects and to obtaining an accurate picture of the extent, characteristics and the patterns of service use of the local homeless population. These data elements are critical to meeting the Congressional requirement for HMIS. Therefore, all providers participating in local HMIS will be required to collect the universal data elements from all homeless client seeking housing or services.**

***See Data Quality Plan***

**Title:** **Minimum Information Security Protocols**

**Policy:** Participating Agencies must develop and have in place minimum information security protocols.

**Purpose:** To protect the confidentiality of the data and to ensure its integrity at the site.

**Scope:** System wide

---

**Responsibilities**

At a minimum, a Participating Agency must adhere to rules, protocols or procedures outlined in the Security Plan which address each of the following:

- Assignment of user accounts
- Unattended workstations
- Physical access to workstations
- Policy on user account sharing
- Client Record Disclosure
- Report generation, disclosure and storage

***See Security Plan***

**Title:** **Access Privileges to System Software**

**Policy:** Participating Agencies will apply the user access privilege conventions set.

**Purpose:** To enforce information security protocols.

**Scope:** System wide

---

**User Access Privileges to HMIS**

All participating users will need an individual agency unique username & password.

- **User Access**: User access and user access levels will be deemed by the Executive Director and/or Agency Administrator of the Participating Agency in consultation with the OHS System Administrator. The Agency Administrator will request new user accounts and conduct password resets within the Administrative function of Service for the application.

- **Agency Administrator Qualifications:** Time, interest, and ability are the biggest factors in determining who should be an Agency Administrator. This title does not necessarily correspond to the agency's organizational chart. The user designated as the Agency Administrator may also enter client data.

- **Username format:** (Recommended) The System Administrator will create all usernames using a systematic approach. For example, the First Initial of First Name and Last Name. Example Jane Smith's username would be JSmith. In the case where there are two people with the same first initial and last name, a sequential number should be placed at the end of the above format. Ex. JSmith2, JSmith3, JSmith4.

- **Passwords:**

    - **Creation:** Passwords are automatically generated from the software when a user account is created. Agency Administrators will communicate the system-generated password to the user.
    - **Use of:** The user will be required to change the password the first time they log onto the system. The password must be between 8 and 16 characters and contain 2 numbers. Passwords are case sensitive and no symbols are permitted for username or password.
    - **Expiration:** Passwords expire every 45 days. A password cannot be re-used until one entirely different password selection has expired.
    - **Termination from Employment:** The Agency Administrator should notify the System Administrator of any HMIS staff termination within one business day.

**Title:** **Unique User ID and Password**

**Policy:** Authorized users will be granted a unique user ID and password.

**Purpose:** In order to ensure that only authorized users will be able to enter, modify, or read data, unique User ID will be issued to every user.

**Scope:** System wide

---

**Standard**

- Each user will be required to enter a User ID with a Password in order to logon to the system
- User Name and Passwords are to be assigned to individuals
- The Password must be more than 8 characters
- The Password must contain at least one uppercase character, one lowercase character, one number, and one non-alphanumeric character
- The Password cannot contain spaces, the word "clarity", the name of the HMIS instance, the user's name or username, "abc", "123", or more than two consecutive characters.
- The Password is case sensitive

**Discretionary Password Reset**

Initially each user will be given a password for one time use only. The first or reset password will be automatically generated by the HMIS System Administrator and will be issued to the User. Passwords will be communicated in written or verbal form. The first time, temporary password can be communicated via email. Only an Agency Administrator or System Administrator can reset an end user's password manually. All users are able to use the "forgot password" function on the login screen to reset a password.

**Forced Password Change**

Forced password change will occur every 180 days once a user account is issued. Passwords will expire and users will be prompted to enter a new password. Users may not use the same password as the three previous passwords.

**Unsuccessful logon**

If a User unsuccessfully attempts to logon four times, the User ID will be "locked out", access permission will be revoked, and the User will be unable to gain access until their password is reset in the manner stated above.

**Title:** **Access Levels for System Users**

**Policy:** Participating Agencies will manage the proper designation of user accounts and will monitor account usage.

**Purpose:** To apply the proper designation of user accounts and manage the use of the accounts.

**Scope:** System wide

---

**Designation of HMIS Users**

User accounts will be created and deleted by the System Administrator under authorization of the Participating Agency's HMIS Agency Administrator or Executive Director.

**User Levels:**
There are 4 levels of access in use in the HMIS system. These levels should be need based. Need exists only for those shelter staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.

1. **Visibility Only:** Access to the system is limited to only viewing data. The user will have no privileges to add, edit, or delete any data within the system.
2. **Agency Staff:** Access to the system includes visibility but also includes ability to add, edit, or delete any data associated with their agency only. Other agency's data can only be viewed.
3. **Agency Administrator:** Access to the system includes visibility, ability to add, edit, or delete any data associated with their agency, and administrative abilities within their agency only.
4. **System Administrator**: Full access to the system.

**Title:** **Access to Data**

**Policy:** Participating Agencies must agree to enforce the user access privileges to the application as stated below.

**Purpose:** To gain understanding that there are many issues involving data

**Scope:** Agency

---

**Responsibilities**

A. **User Access:** Users will be able to view all open/shared data within the HMIS. Users will only be able to modify or edit data entered by users of their own agency. Security measures exist within the HMIS software system, which restrict agencies from editing or changing each other's data.

B. **Raw Data:** All End Users who have been granted access to the HMIS custom reporting tool, Looker, have the ability to download and save client level data onto their local computer. Once this information has been downloaded from the HMIS server in raw format to an agency's computer, this data then becomes the responsibility of the agency. A participating Agency should develop a protocol regarding the handling of data downloaded from the reporting tool.

C. **Agency Policies Restricting Access to Data:** The Participating Agencies must establish internal access to data protocols. These policies should include who has access, for what purpose, and how they can transmit this information. Issues to be addressed include the storage, transmission, and disposal of these data.

**Title:** **Access to Client Paper Records**

**Policy:** Participating Agencies will establish procedures to ensure the security of client paper records.

**Purpose:** To establish internal procedures regarding which staff has access to client paper records and to enforce information security protocols.

**Scope:** Agency

---

**Procedure**

- Identify which staff has access to the client paper records and for what purpose. Staff should only have access to records of clients, which have been referred by Coordinated Intake, that they directly work with or for data entry purposes.
- Identify how and where Client paper records are stored.
- Adhere to HUD Recordkeeping Requirements regarding length of storage and disposal procedure of paper records.
- Develop policy on disclosure of information contained in client paper records.

**Title:** **Physical Access Control**

**Policy:** Physical access to the system data processing areas, equipment and media must be controlled. Access must be controlled for the transportation of data processing media and other computing resources. The level of control is contingent on the level of risk and exposure of risk.

**Purpose:** To delineate standards for physical access.

**Scope:** System wide

---

**Guidelines**

Personal computers, software, documentation and compact discs hall be secured proportionate with the threat and exposure to loss. Available precautions include equipment enclosure, lockable power switches, equipment identification, and fasteners to secure the equipment.

A. **Access to computing facilities and equipment**

All those granted access to an area or to data are responsible for their actions. Additionally, those granting another person access to an area are responsible for that person's activities.

B. **Media and hardcopy protection and transportation**

- Printed versions of confidential data should not be copied or left unattended and open to unauthorized access.

- Media containing client-identified data will not be shared with any Non-Participating Agency for any reason. Authorized employees using methods deemed appropriate by the participating agency may transport HMIS data that meet the above standard. Reasonable care should be used, and media should be secured when left unattended.

- HMIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

**Title:** **Logical Access**

**Policy:** All users will be granted access to the system based on logical need. Need exists only for those shelter staff, volunteers, or designed personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.

**Purpose:** To prevent unauthorized access

**Scope:** System Wide

---

Access to the database and sensitive data resources will be controlled based on the user's needs. Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers.

In order to protect unauthorized access to HMIS, the following measures will be utilized:

- Each Agency will be given an agency specific unique username & password
- Every individual who has access to HMIS will be issued a username & password
- All HMIS system use is internally tracked with an audit trail that shows the information added, edited, deleted, or viewed by the end user
- All computing resources will be protected at all times by a firewall
- Browsers supporting 128-SSL encryption are required to provide encryption of information when information is transferred over the web
- The database server will be encrypted

**Title:** **Right to Deny User and Participating Agencies Access**

**Policy:** Participating Agency or User may be sanctioned, suspended, or system access revoked for suspected or actual violation of the security protocols.

**Purpose:** To outline consequences for failing to adhere to information security protocols.

**Scope:** Agency

---

Serious or repeated violation by Users of the system may result in the suspension or revocation of an agency's access.

- The System Administrator will investigate all violations of security protocols.
- Any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to a formal letter of reprimand, a suspension of system privileges, revocation of system privileges, or legal action.
- Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.
- All sanctions are imposed by the HMIS Data Committee.
- Recommendations or actions of the System Administrator can be appealed to the HMIS Data Committee.

**Title:** **Data Access Control**

**Policy:** Site Technical Administration at Participating Agencies and System Administrator must monitor access to system software

**Purpose:** To indicate the standards and guidelines for data access control for the participating agency.

**Scope:** System wide

---

**Standard**

Agency Administrators at Participating Agencies and the System Administrator must regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access.

Agency Administrators at Participating Agencies must implement discretionary access controls to limit access to HMIS information when available and technically feasible.

Participating Agencies and Systems Administrator must audit all unauthorized accesses and attempts to access HMIS information. Participating Agencies and Systems Administrator also must audit all off-campus accesses and attempts to access HMIS systems. Audit records are captured by HMIS system and System Administrator shall regularly review the audit records for evidence of violations or system misuse.

**Guidelines**

- Each user will have one unique identification code.
- Passwords are the individual's responsibility, and users cannot share passwords.
- Users select and change their own passwords, and must do so at least every 180 days. A password cannot be re-used until 2 password selections have expired.
- Passwords should not be able to be easily guessed or made up. The password format is alphanumeric.

Passwords are case sensitive.

- Any password written down should be securely stored and inaccessible to other persons. Users should not store passwords on a personal computer for easier log on.

**Title:** **Monitoring, Violations, Exceptions, & Termination Rights**

**Policy:** The System Administrator will monitor access to all systems that could potentially reveal a violation of information security protocols.

**Purpose:** To assign responsibility for monitoring of compliance with information security protocols and the process by which Office of Homeless Services will monitor compliance with such policies.

**Scope:** System wide

---

**Monitoring:** Monitoring compliance is the responsibility of the System Administrator in consultation with the Office of Homeless Services and reviewed by the HMIS Data Committee.

**Violations:** The System Administrator and Office of Homeless Services staff will review standards violations and recommend corrective and disciplinary actions. Users should report security violations to their Agency Administrator or System Administrator as appropriate.

**Exceptions:** All exceptions to these standards are to be requested in writing by the Executive Director of the Participating Agency (or designee) and reviewed by the System Administrator as appropriate as well as the Office of Homeless Services staff.

**Exception Violations:** Any exception to the data security policies and standards not approved by the System Administrator is a violation and will be reviewed by the HMIS Data Committee for appropriate disciplinary action that could include recommendation of termination of employment or criminal prosecution.

**Termination Rights:** Participating Agencies may terminate the HMIS Agency Agreement with or without cause upon 30 days written notice to the Office of Homeless Services. The termination of the HMIS Agency Agreement by the Participating Agency may affect other contractual relationships with the Office of Homeless Services. In the event of termination of the HMIS Agency Agreement, all data entered into the Cuyahoga County HMIS will remain an active part of the Cuyahoga County HMIS, and records will remain open, closed, or read only according to the sharing agreement being applied at the time of termination.

**Explanation:** While Participating Agencies may terminate relationships with the Office of Homeless Services HMIS, the data entered prior to that termination will remain part of the database. This is necessary for the database to provide accurate information over time and for that information to be used to guide planning for community services in Cuyahoga County. The termination of the HMIS Agency Agreement may affect other contractual relationships with the Office of Homeless Services.

***See Security Plan***

**Title:** **Data Integrity Controls**

**Policy:** Controls must exist to ensure data remain consistent with their source.

**Purpose:** To delineate the categories of data integrity controls that the Office of Homeless Services & Participating Agencies will apply. To indicate the type of integrity controls required for enforcing and maintaining integrity standards.

**Scope:** System wide

---

Data integrity controls must encompass both manual and electronic processing. Errors, duplications, omissions and intentional alterations should be discovered and investigated. Many data integrity controls will reside within the application or system.

HMIS System maintains an audit trail that will track client-related activity. Any time a client page is added, edited, deleted, or viewed by an end user, that information will be logged.

- The system will enforce referential integrity rules and restraints
- Only authorized personnel are permitted system access
- Only the vendor, Bitfocus Inc., has access to the back-end of the system

| | |
|---|---|
| **Title:** | **Local Data Storage** |
| **Policy:** | Client records containing identifying information that are stored within the Participating Agency's local computer are the responsibility of the Participating Agency. |
| **Purpose:** | To delineate responsibility that Participating Agencies have for client-identifying information stored on local computers. |
| **Scope:** | Participating Agencies |

Participating Agencies shall develop policies for the manipulation, custody and transmission of client-identified data sets. Policies must be documented and include storage format(s) and length of time stored.

**Title:** **Electronic Transmission of Authenticators**

**Policy:** OHS staff and Participating Agencies will not engage in electronic transmission of user ID's and passwords, except for first-time temporary passwords.

**Purpose:** To protect the integrity of the authentication process.

**Scope:** System wide

---

**Standard**

Office of Homeless Services staff and Agency Administrators must be aware of vulnerabilities in the transmission of authenticators.

Authenticators will be transmitted only by telephone, mail, or in person.

**Title:** **Planned Technical Support**

**Policy:** Office of Homeless Services will offer a standard technical support package to all Participating Agencies.

**Purpose:** To describe the elements of the technical support package offered by the Office of Homeless Services.

**Scope:** System wide

---

**Standard**

Office of Homeless Services staff will provide technical assistance to Participating Agencies on use of the application.

Office of Homeless Services staff will provide technical support on a planned schedule with each participating agency.

- Provide general system and program-specific training to all CoC End Users
- Conduct follow-up training as needed
- Develop program specific interview protocol
- Assist in development of program/project workflow
- Provide ongoing technical assistance as needed

The issues for which the Office of Homeless Services is available include:

- **Standard Site Support**
    - Implementation Support
    - Technical Support
    - Reporting Support
    - Training
- **Special Requirements**
    - Program Reports
    - Raw Data Analysis
    - Production of Published Reports

**Title:** **Participating Agency Service Request**

**Policy:** The System Administrator will respond to requests for services that arrive from the Agency's Executive Director or the Agency Administrator.

**Purpose:** To outline the proper methods of communicating a service request from a Participating Agency to the System Administrator.

**Scope:** Participating Agencies

---

To effectively respond to service requests, the System Administrator will require that proper communication channels be established and used at all times.

**Service Request from Participating Agency**

A. Executive Director or Agency Administrator contact the Office of Homeless Services System Administrator

B. Office of Homeless Services System Administrator determines resources needed

C. Office of Homeless Services System Administrator and Bitfocus Inc. develop a mutually convenient service schedule

**Chain of Communication**

Participating Agency Staff - Agency Administrator or Executive Director - Agency Administrator – Agency End Users

Office of Homeless Services System Administrator - Agency Administrator

Office of Homeless Services Staff - System Administrator

Office of Homeless Services System Administrator – Bitfocus Inc

**Title:** **Response Technical Support**

**Policy:** Participating Agencies will receive technical support from the Office of Homeless Services System Administrator on an as needed basis and in the case of unforeseen circumstances that may call for such support.

**Purpose:** To delineate the conditions that justify "response support" and to outline the procedure for communicating the request and for documenting the outcome of such support.

**Scope:** System wide

---

**Standard**

The System Administrator will respond by phone or email within one business day to the Agency Administrator. The System Administrator will only respond to the Agency Administrator or Executive Director.

The System Administrator will respond rapidly to address any problems that impede data entry and retrieval in the HMIS system.

**What conditions call for response?**

Any interference in use of the system

**Communicating the request for rapid response**

All communication should be directed to the System Administrator. The System Administrator will respond via phone or email.

**Documenting the outcome of the support service**

The System Administrator will prepare a brief statement specifying the date, nature of the technical assistance request and outcome of the service. This document will be logged by the Office of Homeless Services System Administrator.

**Title:** **System Administrator Availability**

**Policy:** The System Administrator will be available to each HMIS Agency Administrator and the community of users in a manner consistent with reasonable service request requirements.

**Purpose:** To assist Participating Agencies with data collection and reports, the System Administrator will be available to resolve technical issues

**Scope:** System wide

---

**Standard**

**End Users:** Each user is associated with a primary agency, program or project. Therefore, all password resets and HMIS-related issues should be first directed to the respective agency's HMIS Agency Administrator.

**HMIS Agency Administrators:** Any issues that cannot be resolved or that require additional assistance must be forwarded to the System Administrator only by the HMIS Agency Administrator. The System Administrator will be available for Technical Assistance, questions, and troubleshooting between the hours of 8:00 a.m. and 4:00 p.m. Monday through Friday, excluding city, state, federal holidays, and personal days.

**Contacting the System Administrator**

The System Administrator's contact information will be posted in the HMIS system.

The System Administrator can be emailed at the following address:
nbutina@cuyahogacounty.us

**Training Materials**

Copies of CoC HMIS Training materials are available upon request to the System Administrator. Additional training content is available at learn.bitfocus.com with basic support an technical assistance at get.clarityhs.help

**Title:** **Data Release Authorization and Distribution**

**Policy:** Aggregate data will be available for reporting

**Purpose:** To protect client confidentiality

**Scope:** System wide

---

**Release of data principles**

- Only de-identified aggregate data will be released to Non-Participating Agencies
- There will be full access to view data for all Participating Agencies
- Aggregate Data will be available in the form of an aggregate report or as a raw data set with client identifiers hashed or encrypted
- Aggregate data will be used for research purposes, local reports and may be provided to the public

**Title:** **Right to Deny Access to Client Identified Information**

**Policy:** The HMIS Data Committee retains authority to deny access to all client identified information contained within the system

**Purpose:** To protect client confidentiality

**Scope:** System Wide

---

- No data will be released to any person, agency, or organization that is not an HMIS Participating Agency
- Any request for client identified data from any person, agency, or organization other than a Participating Agency will be forwarded to the Office of Homeless Services for review
- Any outside entity must obtain the written consent of every client contained within the database prior to the release of the data

**Title:** **Quality Control On-Site Review**

**Policy:** The Office of Homeless Services will perform random on-site reviews at the Participating Agency.

**Purpose:** To ensure the integrity and confidentiality of client data

**Scope:** System wide

---

- All Participating Agencies will adhere to the CoC HMIS Policies and Procedures. The management and operations practices at each agency must align with the HMIS Policies and Procedures. The HMIS Lead Agency will determine the exact procedures for on-site reviews

- On-site reviews enable the System Administrator to monitor compliance with the Policies and Procedures Manual and HMIS Agreements

- **On-site reviews include monitoring of Data Quality, Security, and Privacy as outlined in the each of the plans.**

**Title:** **Roles and Responsibilities: Client Grievance**

**Policy:** Clients will contact the Agency with which they have a grievance for resolution of HMIS problems. Agencies will follow their Grievance Procedure to resolve the issue.

**Purpose:** A clear and effective client grievance policy protects the needs of the client and the confidentiality of client data.

**Scope:** Participating Agencies

---

**Standard**

Each Participating Agency is responsible for answering questions and complaints from their own clients regarding the HMIS.

Clients will bring HMIS complaints directly to the Participating Agency with which they have a grievance. Agencies will provide a copy of their Agency Grievance Policy & follow their agency's grievance procedure. An HMIS Policies & Procedures Manual will be issued to the client upon request. Agencies will record all grievances.

Should the client be dissatisfied with the result of a grievance, the agency must allow for an appeal and notify the HMIS System Administrator for further review by the HMIS Lead Agency and HMIS Data Committee.

**Title:** **Agency User Problems**

**Policy:** Participating Agencies will contact the System Administrator to resolve HMIS problems.

**Purpose:** In order for the HMIS to serve as an adequate tool for Participating Agencies and guide for system-wide planning, any HMIS problems must be addressed by the organization with the means to effect system-wide change.

**Scope:** All Participating Agencies

---

**Standard**

The HMIS Lead Agency is responsible for the operation of the CoC HMIS. Any problems with the operation or policies should be discussed with the HMIS Lead Agency.

Participating Agencies will bring HMIS problems to the attention of the HMIS System Administrator. If the System Administrator cannot resolve the problem, the System Administrator will work directly with the HMIS vendor or obtain technical assistance through the HUD AAQ when necessary.

**Title:** **HMIS Data Committee**

**Policy:** An Advisory Committee, representing stakeholders to this project will advise all project activities.

**Purpose:** To define the roles and responsibilities of the HMIS Data Committee.

**Scope:** System wide

---

The responsibilities of the HMIS Data Committee will be apportioned according to the information provided below.

The HMIS Data Committee advises and supports the Cleveland/Cuyahoga County HMIS operations in the following programmatic areas: consumer involvement, quality assurance and accountability. The committee meets on an adhoc basis.

Membership of the HMIS Data Committee will be established according to the following guidelines: 3 or more years of experience with HMIS and a current staff member at a stakeholder agency that enters data into HMIS.

Target for membership will be 5 stakeholders.

There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the project.

The following issues may be covered:

- Planning, decision-making, evaluation and facilitation for the implementation of HMIS
- Coordination and recommendations to assist projects with participation (i.e. resources, workflow, etc)
- Determining and making recommendations on policies and procedures for the HMIS system
- Evaluating potential projects regarding research efforts and linking HMIS with other databases
- Supporting the rights and privacy of homeless persons as it relates to HMIS.
- Selecting additional data elements to be collected by all programs and projects participating in the system
- Review of appeals to grievance decisions and escalations
- Issuing sanctions to violators of security protocols.
    - Sanctions may include but are not limited to a formal letter of reprimand, a suspension of system privileges, revocation of system privileges, recommendation of termination of employment, and criminal prosecution
    - Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked
    - All sanctions can be appealed

**MEMORANDUM OF UNDERSTANDING**
**Participating Agency Agreement**
**For the Cleveland/Cuyahoga County Homeless Management Information System (HMIS)**

This Memorandum of Understanding is entered into by and between the Cleveland/Cuyahoga Office of Homeless Services (OHS), as the HMIS Lead Agency, and _____ (Participating Agency) which provides housing and/or other services to the homeless in Cuyahoga County on this day, _____20__.

**This Memorandum of Understanding represents an agreement to comply with the Policies and Procedures described in detail in the HMIS Policies and Procedures Manual.**

**WHEREAS,** The Cleveland/Cuyahoga County Office of Homeless Services has contracted with Bitfocus Inc. for a client management information system, known as *Clarity™,* for the improved coordination and timeliness of services provided to homeless individuals and families; and

**WHEREAS,** The primary goals of the Homeless Management Information System (HMIS) are to promote the efficient use of the Continuum of Care resources, and coordinate and align community efforts; and inform the development of public policy and strategies to end homelessness; and

**WHEREAS,** The Cleveland/Cuyahoga County Continuum of Care HMIS utilizes a data sharing model among all agencies participating in HMIS.

**NOW THEREFORE, IT IS AGREED AS FOLLOWS:**

***1. The Participating Agency agrees to the following conditions of this MOU:***

a) ***Maintenance of Desktop Hardware/Software and Internet Access.*** The Participating Agency shall maintain the minimum required hardware and software necessary to run *Clarity™* to adequately participate in the HMIS Program. Minimum workstation requirements and browser recommendations are provided in the HMIS Policies and Procedures Manual.

b) ***Security of Data.*** The Participating Agency shall enforce and maintain security of all information stored or reports generated via the *Clarity™* system. The Participating Agency will designate an individual as the HMIS end user and the System Administrator (SA) will assign a Unique ID to the designee accessing the *Clarity™* system. The Participating agency and end user will adhere to all privacy and confidentiality standards outlined in the "HMIS End User Agreement" (*attached hereto*). Specific guidelines will also be given for security settings, which should be maintained on any Internet Browser used to access *Clarity™.* The Participating Agency shall immediately notify the SA within one day of all personnel changes involving those staff authorized to have access to client data in *Clarity™.* Each Participating Agency shall defend and indemnify the Cleveland/Cuyahoga County OHS and the other Participating/Partner agencies from any claims or causes of action arising from the unauthorized release of data.

c) ***Access to Shared HMIS Data.*** All client information will remain available only to HMIS Participating Agencies as part of interagency data sharing designed to facilitate coordinated intake and service delivery. Any agency given authorized access to HMIS data must maintain confidentiality of client records. Per HUD regulations, information collected in HMIS is "Protected Personal Information (PPI)", which means that the individuals' identity and personal information may not be made public. A Participating Agency may not use or disclose the personally identifiable information of any client within HMIS. Data may only be shared with the community in aggregate form.

d) ***Timely Input of Client Data.*** The Participating Agency is responsible to input all client data into the *Clarity ™* system in a timely manner as specified in the HMIS Data Quality Plan. The Participating Agency will enter information into HMIS according to the required standards and will ultimately strive for real-time, or close to real-time, data entry.

e) ***Data Quality and Compliance.*** Each Participating Agency is responsible for its staff and agency compliance relative to requirements for data entry and use of HMIS. Each Participating Agency is responsible for generating its own reports; Additional training and support are provided upon request.

***f)*** ***Costs - Annual Support Fees and User Licenses.*** The Cleveland/Cuyahoga County Continuum of Care (CoC) shall pay for User Licenses and Annual Support Fees for each Participating Agency's use. It is possible that each Participating Agency will need to agree to pay a minimal renewal fee directly to the vendor if future funding is not attained by the CoC.

***2. The Cleveland/Cuyahoga County Office of Homeless Services agrees to the following responsibilities:***

a) ***Security of Data on Application and Database Server*s.** Bitfocus Inc. shall keep secure all client data in the *Clarity ™* system. This shall prohibit access by individuals who are not registered with the System Administrator (SA) and therefore, are unauthorized to receive Participating Agency and client information through any and all means. All changes to access codes, passwords, and personnel registration for the *Clarity ™* system will be handled through the Agency Administrator and then the SA. The Cleveland/Cuyahoga County Office of Homeless Services and the Continuum of Care shall not be held liable for any breach in security related to changes in authorized Participating Agency personnel if the agency has not notified the SA of these changes. The SA will provide ongoing auditing and monitoring of compliance with data security and policy standards.

b) ***Documentation/Manual on use of Clarity ™*** .The software vendor, Bitfocus, will provide, maintain, and update, on-line resources regarding the use of the *Clarity ™* system.

c) ***Training.*** The Office of Homeless Services shall provide initial and ongoing training opportunities of HMIS Participating Agency personnel on use of the *Clarity ™* software.

d) ***Help Desk Support.*** The System Administrator will provide support between the hours of 8am and 4pm on regular business days. The Systems Administrator will acknowledge all situations within one business day.

e) ***Costs.*** Access to the *Clarity ™* system will be provided free for the period of one year. At the end of the first year, an agency may continue to use the system for a minimal Annual Support Fee, if the Continuum does not secure future funding. The Cleveland/Cuyahoga County Continuum of Care shall determine, in consultation with the vendor, the per agency cost. Costs shall be documented and itemized.

**Terms and Termination**: The initial term of this agreement is **one year**; commencing _____through _____. The agreement will automatically renew for an additional one-year period at the expiration of the then current term, unless either party requests a review or revision. The agreement may be terminated at any time by the Office of Homeless Services with written notification to the Participating Agency. Within 14 days of termination, the Participating Agency must delete all HMIS data in its possession. Upon termination of this agreement, notwithstanding anything in the agreement to the contrary, the OHS and Continuum of Care shall have the continuing right after the termination of this agreement to retain and use a copy of Participating agency's data which was shared during the course of this agreement

**PARTICIPATING AGENCY:**

**Agency Name**
**Agency Address**
**Agency City, State, Zip Code**

**IN WITNESS WHEREOF, the parties hereto have caused this MOU to be executed and delivered by their duly authorized representatives as of the date set above.**

By: _____
Cleveland/Cuyahoga County Office of Homeless Services

By: _____
Participating Agency

# HMIS
# PRIVACY PLAN

Cleveland/Cuyahoga County Continuum of Care

## HMIS Privacy Plan

### Overview

In 2004, the U.S. Department of Housing and Urban Development (HUD) released standards for the Homeless Management Information System which specified the responsibilities of each HMIS Lead Agency and Participating Agencies.

This document describes the Privacy Plan of the Cleveland/Cuyahoga County Continuum of Care (CoC). All Participating Agencies must adhere to the policies and procedures outlined in this plan. We have adopted a Privacy Plan which supports an open data sharing structure of client-level data among CoC Providers to enable coordination between partners and facilitate effective service deliver to clients.

The core tenet of the Privacy Plan is the Privacy Notice. This Privacy Notice describes how client information is used and disclosed. It also explains how a client might access their information. Each agency is asked to adopt this document to ensure that all Participating Agencies are governed by the same standards of client privacy protection.

All amendments to the Privacy Plan are approved by the HMIS Data Committee for the Cleveland/Cuyahoga County Continuum of Care.

| Privacy Plan Documents | Description | Use by Agency |
|---|---|---|
| Privacy Notice | This is the main document of the Privacy Plan. This notice outlines the minimum standard by which an agency collects, utilizes and discloses client information. | REQUIRED – Participating Agencies must adopt this Privacy Notice to ensure that minimum HUD standards are being met. |
| Privacy Posting | This posting explains the reason for collecting personal information and provides the client with proper notification of the actual Privacy Policy. | REQUIRED – Participating Agencies must adopt and utilize the Privacy Posting. This document must be posted at every location where a client intake occurs. This must also be posted in publicly accessible areas at each site. |
| Client Information Release Authorization | An informed client consent protocol and notation in the client's HMIS record of their consent to provide PII provides documentation that the client has been informed of the privacy notice, individual rights, the sharing of data throughout the CoC. | REQUIRED – Each Participating Agency is required to inform clients of the Privacy Policy and obtain consent from each individual and household member via verbal approval or signed written consent prior to entering any client information into HMIS. Clients who choose not to have their data entered into HMIS will not be refused services. |
| Client Consent to Rescind Participation | Execution of this form allows the client to document their refusal of HMIS participation and the sharing of their personal data from the time the form is executed. | REQUIRED – Each Participating Agency must inform each client of their right to refuse participation at any time and must provide this form upon request. |

**User Responsibilities**

A client's privacy is upheld only to the extent that the users and direct service providers protect and maintain the client's information. Anyone that has direct interaction with a client or their data is responsible for protecting all client-level information entered into HMIS.

Users and Intake Staff must:

- Understand and communicate to clients the contents of the HMIS Privacy Notice
- Provide each client with a copy of the Privacy Notice at HMIS intake or project entry, whichever occurs first
- Address any client concerns or questions either directly or via referral to appropriate manager
- Comply with the Privacy Notice and protect the privacy of all client data entered into HMIS

**Participating Agency Responsibilities**

The HUD HMIS Standards clearly state each agency's responsibility for upholding client privacy. This Privacy Plan and the Privacy Notice provide guidance on the minimum standards by which agencies must operate in order to participate in the HMIS. Meeting these standards is a requirement for participation. Agencies must adopt the Privacy Notice prior to entering client information into HMIS.

Participating Agencies must:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in the Privacy Plan and Privacy Notice (i.e. Substance Abuse Providers, Legal Service Providers, HIPPA Covered Agencies)
- Adopt and uphold the Privacy Notice which meets the HUD standards. Modifications to the Privacy Notice will be approved by the HMIS Data Committee
- Ensure that all clients are aware of the Privacy Notice and have access to it.
- Appoint a Site Agency Administrator who will also serve as the HMIS Security Officer. This individual is responsible for ensuring all aspects of client privacy as it relates to data collection and HMIS.
- Provide participant consent form(s) and/or explain privacy policy information to clients and document client's consent as required by the Partner Agency, state, and/or federal laws and the HMIS standards **prior** to entering client information into the HMIS database.
- Cuyahoga/Cleveland collects, utilizes and shares client PII in an **INFORMED** consent environment. The burden rests with the Partner Agency End-user or intake counselor to inform the client about the purpose and function of HMIS data before asking for consent.
    - If the client does not provide consent the Partner Agency End-user is required to maintain utilization documentation of the client's participation via an alternative data systems or database. If PII are collected and maintained in an alternative and/or comparable database, that alternative database must adhere to all HMIS Privacy, Security and Data Quality standards.
- As part of informed consent, a privacy notice must be posted in the intake area explaining:
    - the reasons for collecting the data,
    - the client's rights with regards to data collection, and
    - any potential future uses of the data.

- The agency must also make available the relevant CoC & HMIS Governance Policies & Procedures and a list of agencies participating in Cleveland/Cuyahoga County's HMIS Project.
- Be aware of specific protections afforded under Federal Law for persons receiving certain types of services such as domestic violence services, HIV or AIDS treatment, substance abuse services, or mental health services.
- Offer the client the opportunity to input and share additional client information with other Provider Agencies beyond basic identifying data and non-confidential service information.
- Obtain client consent for additional client information and communicate what information will be shared and with whom.
- Data may be collected and entered into HMIS only when that data is expected to be useful for organizing, providing, or evaluating the delivery of housing or housing-related services.
- Data used for research or policy evaluation by non-participating HMIS agencies will be shared only after the data has been thoroughly de-identified; this includes removing names, contact information, and removing descriptions or combinations of characteristics that could be used to identify a person.
- Provide verbal explanation of Cleveland/Cuyahoga County CoC HMIS and arrange for, when possible, a qualified interpreter or translator for a client not literate in English or having difficulty understanding the consent form(s).
- End-users are prepared to explain (to the client) security measures used to maintain confidentiality.
- Enter all minimum data required by the HMIS. Client data, including client identifiable and confidential information, may be restricted to other Provider Agencies. Each Agency Executive Director is responsible for their agency's internal compliance with the HUD HMIS Data Standards.

HMIS System Administrator

- Adopt and uphold the Privacy Notice which meets the minimum HUD standards.
- Train and monitor all Participating Agencies regarding data integrity and protection of client information
- Monitor agencies to ensure adherence to the Privacy Notice
- Respond to each "Request to Rescind Participation" and make appropriate changes in the HMIS live system.

# HMIS Privacy Posting/Data Collection Notice

## CLEVELAND/CUYAHOGA COUNTY CONTINUUM OF CARE
## HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)


**THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.**

***PLEASE READ IT CAREFULLY***

### Our Duty to Safeguard Your Protected Information

This agency is an HMIS participating provider and collects information about those who access homeless services. When we meet with you we will ask you for information about you and any member of your household. This information will be entered into a computer program called the Homeless Management Information System (HMIS).

Although HMIS helps us to keep track of your information, individually identifiable information about you is considered **"Protected Information". We are <u>required</u> to protect the privacy of your identifying information and any other information you provide.**

We are also required to follow the privacy practices described in this Notice, although the Cleveland/Cuyahoga County Continuum of Care reserves the right to change our privacy practices and the terms of this Notice at any time. You may request a copy of the new notice from any HMIS Agency.

### How We May Use and Disclose Your Information

Cleveland/Cuyahoga Continuum of Care HMIS data will reside in one central database. Basic client intake information may be shared with agencies participating in the CoC HMIS or conducting research/analysis in order to gauge service delivery and make accessing services from other agencies easier and quicker for you.

We use and collect information for a variety of reports on homeless services specifically.
For uses beyond reports, we must have your written consent unless the law permits or requires us to make the use or disclosure without your consent.

**You have the right to obtain services even if you choose NOT to participate in HMIS.**

*If you decline to have your information entered into HMIS, you must notify your case manager verbally or in writing.



**HMIS PRIVACY POSTING**

**CLEVELAND/CUYAHOGA COUNTY CONTINUUM OF CARE**
**HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)**

**_____**
**[AGENCY NAME]**

**We collect personal information directly from you for reasons detailed in the Cleveland/Cuyahoga County Continuum of Care HMIS Privacy and Data Collection Notice. We may be required to collect some personal information by law or by organizations that give us money to operate this facility/program/project. Other personal information that we collect is important to provide quality services, to improve services for homeless individuals/families, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate. If you would like to see the full version of the HMIS Privacy and Data Collection Notice, our staff will provide you with a copy. You have the right to obtain services even if you choose NOT to participate in HMIS.**

## Cleveland/Cuyahoga County HMIS Consent and Release

When you request or receive services from the Cuyahoga County Continuum of Care (CoC), information is collected about you and your household. This information is then entered into the Cleveland/Cuyahoga County Homeless Management Information System (CCHMIS). The CCHMIS is used by over 40 local, social service agencies to coordinate service delivery.

**What type of information is collected?**

- Basic identifying information for you and each member of your household (may include name, SSN, date of birth, gender, race, ethnicity, household information, phone numbers, military veteran status, disability status)
- Income information (sources and amounts of household income, employment information, work skills)

What happens to the information collected?

- With your approval, information collected is shared with other service agencies participating in HMIS for the purpose of coordinating service delivery, identifying needs and tracking outcomes.
- CCHMIS aggregate data (non-identifying) may be used for community reports and shared with Federal, State, local agencies and other institutions for the purpose of research and analysis. Client information is only shared with authorized persons.

*NOTE: CCHMIS uses many security protections to ensure confidentiality and only agencies that use CCHMIS can access this program. All partner agencies adhere to strict security policies to protect your privacy. HMIS software is highly secure.*

**Why should you agree to have your information shared with other agencies that use Cuyahoga County HMIS?**

The benefits to sharing your information in HMIS are as follows

- Reduce the number of visits to other agencies and forms completed
- Identify other services or programs you may be eligible for
- Better coordinate services for you and your household

### CLIENT INFORMED CONSENT/RELEASE OF INFORMATION AUTHORIZATION

*You have the option to cancel access to personal information that you are providing about yourself and your minor children at any time. If you choose to cancel previous authorization, you must do so in writing. Please contact intake staff at the CoC Agency you're currently working with to formally rescind authorization. Please note that canceling authorization (rescinding authorization) will only impact future release of client information.*

☐ ***AUTHORIZATION OF CONSENT:*** *All information may be shared with authorized personnel in participating and partner agencies relative to the Cleveland/Cuyahoga County: Your release of information and authorization is valid for three (3) years.*

☐ ***REFUSAL of CONSENT:*** *I understand that I am not required to sign this authorization and that if I do not want this information disclosed; my option is not to sign this authorization. Furthermore, I understand that services will not be withheld if I refuse consent.*

SIGNATURE of Client, Guardian or Head of Household _____ DATE _____

PRINTED NAME _____

SIGNATURE of AGENCY WITNESS _____ DATE _____

**ADDITIONAL HOUSEHOLD MEMBERS:**

| | | | |
|---|---|---|---|
| PRINTED NAME OF CLIENT | Relationship to HOH | PRINTED NAME OF CLIENT | Relationship to HOH |
| PRINTED NAME OF CLIENT | Relationship to HOH | PRINTED NAME OF CLIENT | Relationship to HOH |
| PRINTED NAME OF CLIENT | Relationship to HOH | PRINTED NAME OF CLIENT | Relationship to HOH |
| PRINTED NAME OF CLIENT | Relationship to HOH | PRINTED NAME OF CLIENT | Relationship to HOH |

**Consent to Rescind Participation in HMIS**
**Cleveland/Cuyahoga County Continuum of Care**

**Last Name:** _____

**First Name:** _____

**Middle Initial:** _____

**Date of Birth:** _____

**Social Security Number:** _____

I, _____, choose to no longer participate in the HMIS. I understand that by signing this form, my file will be deleted and no longer accessible to HMIS Partner Agencies.

_____ _____
Client's Authorizing Signature Date

I, _____, as the Legal Guardian of the below listed individuals, rescind their participation in the HMIS.

_____ _____
Name Date of Birth

_____ _____ _____
Name Date of Birth Guardian's Signature

_____ _____
Name Date of Birth

_____ _____
Name Date of Birth

*FOR AGENCY USE ONLY:*

Agency Name Where Form Completed:_____

Agency Representative Working with Client: _____

Date Submitted to HMIS Systems Administrator: _____

**Clarity Unique** ID(s): _____

# HMIS
# SECURITY PLAN

Cleveland/Cuyahoga County Continuum of Care

**HMIS Lead Agency**

On behalf of the Cleveland/Cuyahoga County Office of Homeless Services (OHS), the System Administrator will serve as the HMIS Security Officer whose duties include:

- Review of the Security Plan annually and at the time of any change to HMIS data or technical requirements issued by HUD. The Security Officer will work with the HMIS Data Committee to review, modify and approve any necessary changes to the Security Plan
- Conduct agency specific security audits on an annual basis
- Respond to any security questions, requests or breaches to the HMIS
- Provide Participating Providers with HMIS security information and updates. Current listing of HMIS Security Standards will be distributed at each quarterly HMIS Training Sessions

**Participating Agencies**

Each participating agency must conduct a criminal background check on each of its Partner Agency HMIS Administrators and Security officers at its own expense. The Partner Agency's Executive Director will evaluate the results of the criminal background checks for any concerns. To protect the security and integrity of the HMIS system and safeguard the personal information contained therein, the Partner Agency's Executive Director must consider the results of the background check on a case-by-case basis.

a. An individual whose background raises concerns about whether s/he may sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may not initially be given administrative-level access to HMIS.
b. An individual whose background raises concerns about whether s/he may sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may be enrolled as an HMIS End-user. After at least one year, if the individual demonstrates through proper and safe use of HMIS that the individual is reliable and trustworthy, they may apply to become a Technical Administrator.
c. The results of the background check must be retained in the subject's personnel file by the Technical Administrator.
d. A background check may be conducted only once for each person unless otherwise required

Each Participating Agency must designate a Site Agency Administrator who will also serve as the Site Security Officer whose duties include:

- Ensuring that the agency is adhering to the HMIS Security Plan
- Communication to the System Administrator of any requests, notification of misuse and security breaches.
- Participating in security training offered by the Cleveland/Cuyahoga County Office of Homeless Services.

HMIS End User Requirements:

a. Log-off the HMIS database and close the Internet browser before leaving a work terminal.
b. Log-off the HMIS database and close the Internet browser prior to surfing the Internet.
c. Never leave an open HMIS database screen unattended.
d. Passwords must not be saved on the computer or posted near the workstation.

e. Immediately notify the designated Agency Administrator or the HMIS Coordinator of any suspected security breach.
f. Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.
g. PC Access (visual) — Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized Partner Agency staff members or volunteers and utilize visibility filters to protect client privacy.

**Annual Security Monitoring**
The OHS System Administrator will complete an annual security audit to ensure compliance relative to the HMIS Security Requirements. OHS will conduct a site visit which will include completion of a security checklist to demonstrate that each of the security standards is fully implemented.
***See HMIS Security Audit Checklist***

**Security Awareness and Training Follow-Up**
All users must receive security training prior to accessing the HMIS. The OHS System Administrator provides security training in tandem with the HMIS End User Training on a quarterly basis.

**Reporting Security Incidents**
All HMIS End Users are required to report any instances of suspected misuse of the system, unauthorized access, security breach or noncompliance to their Site Agency Administrator/Security Officer. Each Participating Agency's Security Officer is required to immediately notify the System Administrator of any incident.

**Violations:** The System Administrator, Office of Homeless Services staff, and the HMIS Data Committee will review standards violations and recommend corrective and disciplinary actions.

**Audit Controls**
Bitfocus Inc. maintains an accessible audit trail within Clarity that allows the System Administrator to generate reports to monitor user access and activity. The System Administrator will monitor audit reports for any apparent security issues. Furthermore, each Site Agency Administrator is required to run audit reports on all HMIS staff annually.

**System Security**
Each Participating Agency must apply system security provisions to all the systems where personal protected information (PPI) is stored, including but not limited to, networks, desktops, laptops, mainframes and servers.

**User Authentication**
Access to the database and sensitive data resources will be controlled based on the user's needs. Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers.

The System Administrator, upon request from the Site Agency Administrator or Executive Director, will grant access to End Users with a completed/signed copy of the End User License Agreement. The System Administrator will provide each End User with a username and password to access HMIS. Passwords must be at least eight characters in length. The username and password, unique to each individual End User, may not be transferred to other staff.

Written information pertaining to user access may not be stored or displayed in any public or publicly accessible location. Users must not log on to more than one workstation at a time.

**Data Access & Password Policies**

a. The Agency Administrator contacts the HMIS System Administrator to set up a new End-user and provides a temporary password.
b. The Agency Administrator communicates this password to the new End-user.
c. The End-user must change the password after initially logging correctly into the database. Never transmit End-user identification and computer-generated passwords together in one email, fax, telephone call, or other means of communication.
d. The End-user creates a ***unique*** password larger than 8 characters with a minimum of one uppercase character, one lowercase character, one number, & one non-alphanumeric character. The password should not contain spaces. The End-user ***DOES NOT*** use a password used for other purposes; this password must be unique**.**
e. Passwords shall not include the End-user name, the HMIS name, or the HMIS Vendor's name. Passwords shall not include spaces, "abc", "123", or more than two consecutive characters.
f. Password is case sensitive.
g. Passwords should be changed every 180 days.
h. End-users must create a new password that is different from the original (expiring) password. End-users cannot use the same password as the previous three passwords.
h. Unique Passwords -- User IDs are individual, and passwords are confidential. No individual should ever use or allow the use of a User ID that is not assigned to that individual, and user-specified passwords should never be shared or communicated in any format.
i. Protection of downloaded HMIS files:
   Cleveland/Cuyahoga County Lead Agency assumes **no** responsibility for the management, protection, and transmission of client-identifying information stored on local agency computers, agency files, and reports.
    1. Partner Agency is responsible for any file or report downloaded from HMIS.

**Virus Protection and Firewalls**

Each Participating Agency must install and maintain virus protection software on each computer or network with current virus definitions and regularly scheduled updates.

Each Participating Agency must protect HMIS from malicious intrusion via an active firewall on either each computer or the network.

Any workstation accessing HMIS shall have antivirus software run the current virus definitions every 24 hours and full-system scans a minimum of once per week.

**Physical Access to HMIS Data**

Participating Agencies must staff computers located in public areas that are used to collect HMIS data at all times. When workstations are not in use steps should be taken to ensure that the computer and data are secure and not accessible to unauthorized persons. Each computer must activate a screen-saver password which is set to turn on when the computer is unattended or has not been in use during a reasonable amount of time (i.e. 10 minutes).

**Hard Copy Security**
Participating Agencies must secure any paper or other hard copy containing personal protected information (PPI) that is either generated for or by HMIS, including but not limited to reports, intake forms and signed consent forms. Any document consisting of PPI must be supervised at all times when in a public area. PPI must be stored in a secure area.

**Hard copies of forms or data generated via HMIS will be treated in the following manner:**

- Records shall be kept in individual locked files or in rooms that are locked when not in use
- When in use, records shall be maintained in such a manner as to prevent exposure of PPI to anyone other than the user directly responsible for reviewing or entering the information into HMIS
- Staff shall not remove records or information containing PPI from the assigned site without permission from appropriate supervisory staff
- Media containing client-identified data will not be shared with any Non-Participating Agency for any reason. Authorized employees using methods deemed appropriate by the participating agency may transport HMIS data that meet the above standard. Reasonable care should be used, and media should be secured when left unattended
- Staff are responsible for ensuring that records are maintained in a secure location (locked drawer or file cabinet) and must not disclose any PPI information contained in those records
- Forms, faxes, reports or other documents containing PPI must not be left unattended
- Fax machines and printers shall be kept in secure locations
- HMIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable

**Database Integrity**

Any unauthorized access or modification to computer system information or interference with normal system operations will result in immediate suspension of licenses and access to HMIS by the Cleveland/Cuyahoga County Office of Homeless Services.

The System Administrator, OHS Staff, and the HMIS Data Committee will investigate and review all potential violations of any security protocols. Any End User found to be in violation of security protocols will be subject to sanctions. Individuals may be subject to disciplinary action by their employer.

**Disaster Recovery**

Cleveland/Cuyahoga County Continuum of Care data is stored by Bitfocus Inc. in a secure and protected offsite location with duplicate back-up. In the event of disaster, the System Administrator will coordinate with Bitfocus Inc. to ensure the HMIS is functional and data restored. The System Administrator will be responsible for communication of information and updates to Participating Agencies.

Bitfocus Inc.'s Disaster Recovery Plan is located below.

**Security Audits**
The Participating Agency Security Officer is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the Agency's control.

The participating Agency Security Officer is responsible for preventing inadvertent release of confidential client-specific information through physical, electronic, or visual access to the workstation.

Each participating Agency Security Officer is responsible for ensuring their agency meets the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards. Partner Agencies will conduct a thorough review of internal policies and procedures regarding HMIS.

To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available via a secure network.

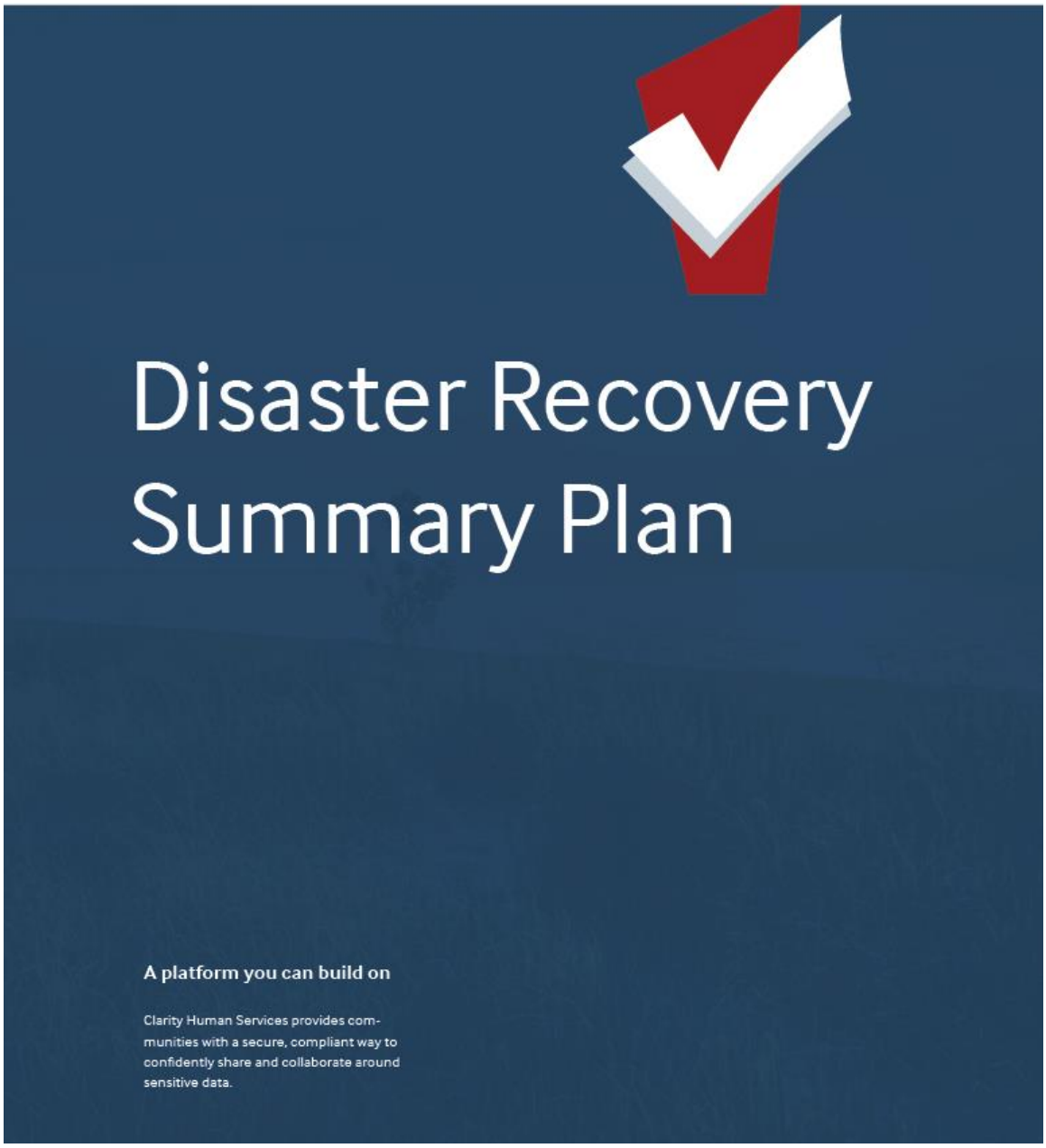
End-users shall commit to abide by the governing principles.

**Secure Archival**
Each Participating Agency shall retain copies of all documents containing PPI in accordance with the HUD Recordkeeping Requirements. These documents must be in a secure area, locked and not accessible to the public.

## HMIS SECURITY AUDIT CHECKLIST

**AGENCY NAME**

| Requirement | Description | Response | Assessment | Action Needed |
|---|---|---|---|---|
| Data Collection | Does the agency have a data collection form and/or protocol that captures the HUD required Universal and Program Specific data elements? | YES | **Agency:**<br>____Y ____N Has a data collections form protocol<br>____Y ____N Is capturing Universal Data Elements<br>____Y ____N Is capturing Program Specific Data Elements<br>____Y ____N Monitors data quality internally<br><br>**Users:**<br>____Y ____N Have been trained on data collection protocol | |
| | | NO | No updated data collections protocol | |
| Privacy: Posted Notice | Does the agency have the HMIS Notice of Privacy Practices posted at every place where intake occurs? | YES | ____# of intake locations _____# of posted notices<br>____Y ____N Copy of full Privacy Notice/Policy is available upon client request | |
| User Authentication | Does the agency abide by the HMIS policies for unique users names and passwords? | YES | ____Y ____N Agency abides by HMIS Policies and Procedures<br>_____ Number of HMIS users at agency<br><br>All HMIS end users at the agency are aware that they should<br>____Y ____N NEVER share usernames and passwords<br>____Y ____N NEVER keep usernames/passwords in public locations<br>____Y ____N NEVER use their internet browser to store passwords<br>____Y ____N All users have signed an HMIS User Agreement | |
| | | NO | Agency does not abide by HMIS user authentication policy | |
| Hard Copy Data | Does the agency have procedures in place to protect hard copy **Protected Personal Information (PPI)** generated from or for HMIS? | YES | Agency has a procedure for hard copy Protected Personal Information (PPI) that includes…<br>Security of hard copy files<br>____Y ____N Locked drawer/file cabinet<br>____Y ____N Locked office | |
| | | NO | Agency does not have procedure for hard copy PPI | |
| PPI Storage | Does the agency dispose of or remove identifiers from a client record after a specified period of time? (HUD minimum standard: 7 years after PPI was last changed if record is not in current use) | YES | Agency has a procedure for removal and storage of PPI<br>____Y ____N Secure disposal of records/reports (shredding, etc.)<br>____Y ____N Secure Archival of files/reports | |
| | | NO | Agency does not have a procedure for removal and storage of PPI | |
| Virus Protection | Do all computers have virus protections with automatic update? (this includes non-HMIS computers if they are networked with HMIS computers | YES | ____Y ____N Random check of several computers for Virus software<br>____Y ____N Updated version of Virus software (less than 30 days)<br>*(May be verified via Certificate of AntiVirus Software or PC check)* | |
| | | NO | No Virus protection installed | |
| Firewall | Does the agency have a firewall on the network and/or workstation(s) to protect the HMIS systems from outside intrusion? | YES | Single computer agencies:<br>____Y ____N Individual workstation has firewall<br><br>Networked (multiple computer) agencies:<br>____Y ____N Network firewall | |
| | | NO | Individual workstation or network firewall not active | |
| Physical Access | Are all HMIS workstations in secure locations or are they manned at all times if they are in publicly accessible locations? (This includes non-HMIS computers if they are networked with HMIS computers.) | YES | All workstations are:<br>____Y ____N In secure locations (locked ofcs.) or manned at all times<br>____Y ____N Using password protected screensavers<br><br>All printers used to print hard copies from the HMIS are:<br>____Y ____N In secure locations<br><br>Data Access:<br>____Y ____N Users may access HMIS from outside the workplace<br>____Y ____N If yes, Agency has a data access policy | |
| | | NO | Not all workstations are manned at all times or are in secure locations. | |
| Data Disposal | Does the agency have policies and procedures to dispose of hard copy PPI or electronic media? | YES | ____Y ____N Agency shreds all hard copy PPI/Identifying info before disposal<br><br>Process for disposal of…<br>____Y ____N Disks<br>____Y ____N CD's<br>____Y ____N Computer Hard Drives<br>____Y ____N Other media (tapes, jump drives, etc.) | |
| | | NO | The agency does not have policies and procedures for data disposal. | |


Disaster Recovery
Summary Plan
A platform you can build on
Clarity Human Services provides communities with a secure, compliant way to confidently share and collaborate around sensitive data.

# Bitfocus Disaster Recovery Plan Summary Document

*Note: One of the objectives of our Information Security Department is to establish an IT Disaster Recovery Plan. This Disaster Recovery Plan document was created to assist Bitfocus in the development of consistent and cohesive IT Disaster Recovery Plans. This is a summary document which omits key infrastructure references to protect our Information Security Infrastructure.*

## Introduction

The purpose of this summary is to document a Disaster Recovery Plan that addresses information resources as they may be affected in the event of a disaster. This document is meant to minimize any of these effects, and enable Clarity Human Services to either maintain, or quickly resume, mission-critical functions. This Disaster Recovery Plan also serves as the primary guide for Bitfocus, Information Technology Services Department in the recovery and restoration of the information technology systems in the event that they are damaged or destroyed as a result of a disaster.

### Document Overview

The Disaster Recovery Plan is composed of numerous sections documenting the resources and procedures to be used in the event that a disaster occurs at the data center, which is located at Flexential in Las Vegas, Nevada. Separate sections are devoted to the specific recovery procedures for each supported application or platform. Also included are sections documenting the personnel requirements that are necessary to perform each recovery task. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the very sensitive nature of the information contained in the plan, this summary omits several key references.

**PERSONNEL AUTHORIZED TO DECLARE A DISASTER OR RESUME NORMAL OPERATIONS**

Robert Herdzik, Founder & CEO
Jeffrey Ugai, Cheif Operating Officer
Tauri Royce, Vice President of Customer Experience

## Disaster Recovery Plan Summary

### Plan Activation

This plan will be activated in response to internal or external threats to the Information Technology Systems of Bitfocus Internal threats could include fire, bomb threat, loss of power or other utility or other incidents that threaten the staff and/or the facility. External threats include events that put the facility in danger. Examples might include severe weather or a disruptive incident in the community. Once a threat has been confirmed, the plan management team will assess the situation and initiate the plan if necessary.

### Resumption of Normal Activities

Once the threat has passed, equipment will be repaired and/or replaced, and/or a new data center will be transitioned. The disaster recovery team will then assess the situation; If the disaster has expired, the team will resume normal operations.

### Plan Objectives

The primary objectives of this plan are to protect Silver Spur Systems' computing resources, to safeguard the vital records of which Bitfocus is the custodian, and to guarantee the continued availability of essential IT services. The role of this plan is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data center and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in IT capabilities. This plan assumes the most severe disaster, the kind that requires moving computing resources to another location. Less severe disasters are controlled at the appropriate management level as outlined in this plan.

The basic approach, general assumptions, and possible sequence of events that need to be followed are stated in the plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The plan is a roadmap from disaster to recovery. Due to the nature of the disaster, the steps outlined may be skipped or performed in a different sequence. The general approach is to make the plan as threat independent as possible. This means that it should be functional regardless of what type of disaster occurs.

For the recovery process to be effective, the plan is organized around a team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery mode. The leader of each team and their alternates are key personnel. IT staff will be assigned to multiple teams with specific assignments made according to knowledge, experience and availability. It is also assumed vendors and knowledgeable personnel will be actively enlisted to help during a recovery situation.

The plan represents a dynamic process that will be kept current through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the plan will be revised to reflect the current IT environment.

## Disaster Recovery Phases

The disaster recovery process consists of four phases. They are:

- Phase 1: Disaster Assessment
- Phase 2: Disaster Recovery Activation
- Phase 3: Alternate Site/Data Center Rebuild
- Phase 4: Return Home

### Phase 1: Disaster Assessment

The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed. Cooperation with Flexential emergency personnel is critical.

### Phase 2: Disaster Recovery Activation

This phase begins if the decision to move primary processing to a location is made. The Disaster Recovery Management Team will assemble at the command center and call upon team members to perform their assigned tasks. The most important function is to fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternate location, Phase 2 is complete.

### Phase 3: Alternate Site Operation/Data Center Rebuild

This phase involves continuing operations at the alternate location. In addition, the process of restoring the primary site will be performed.

### Phase 4: Return Home

This phase involves the reactivation of the primary data center at either the original or possibly a new location. The activation of this site does not have town be as rushed as the activation of the alternate recovery center.

At the end of this phase, a thorough review of the disaster recovery process should be taken. Any deficiencies in this plan can be corrected by updating the plan.

# Key Disaster Recovery Activities

## Declaring a Disaster

Declaring a disaster means:

1. Activating the recovery plan
2. Notifying team leaders & staff
3. Notifying key management contacts
4. Notifying affected customer contacts
5. Securing a new location for the data center
6. Ordering and configuring replacement equipment
7. Reconfiguring the network
8. Restoring Virtual Machine infrastructure from onsite or offsite Backup
9. Keeping management informed
10. Keeping customer contacts informed

## Disaster Decision Tree

| Event | Decision |
|---|---|
| Data Center destroyed | Activate disaster recovery plan |
| Data Center unusable for MORE than 2 days | Activate disaster recovery plan |
| Data Center unusable for 2 days or LESS | Management Team performs an assessment |
| Network down | Management Team performs an assessment |
| Environmental problems (A/C, power, etc) | Management Team performs an assessment |

| Decision Point | Actions | | | | Category |
|---|---|---|---|---|---|
| **1. Incident occurs** | 2. Alarm sounds | 3. Begin evacuation | 4. Ensure all employees evacuated | 5. Meet in designated area | Initiation |
| **7. Determine if incident is real** | 8. If no, then | 9. Recovery plan is not activated | 10. Return to normal operations | 12. Evaluate evacuation | Determination |
| | 8. If yes, then | 9. Switch call handling to an alternate location | | | Determination |
| **10. Determine scope of incident and assess damage after building access is allowed** | 11. If small scope with no to minimal damage, then | 12. Return and begin clean up and monitor repairs | 13. Return calls | 14. Return to normal operations | Short Evacuation Required |
| | 11. If moderate to large scope or moderate to severe damage, then | 12. Activate alternate computer processing site | 13. Activate recovery team | 14. Notify management and employees of of situation | Moderate to Severe Damage to Data Center or Infrastructure |
| **16. Assess damage** | 17. If damage is moderate and will be able to return in 30 days or less | 18 Complete repairs as necessary while operating at alternate site | 19. Return to data center | 20. Return to normal operations | Moderate Severe Damage to Data Center or Infrastructure |
| | 17. If more than 30 days, locate to new facility | 18. Order supplies and equipment | 19. Set up and operate at new facility while completing repairs | 20. Return to normal operations | Severe Data to Data Center or Infrastructure |

# Recovery Time Objectives (RTO)

The Recovery Time Objectives reflect the estimated recovery times based on current configurations and operations.

| Network Service | Recovery Goal |
|---|---|
| LAN (Local Area Network) | 2-3 days estimate |
| WAN (Wide Area Network) | 2 days estimate |
| Internet | 2 days estimate |

| Application Recovery Tier | Recovery Goal |
|---|---|
| Infrastructure Servers | Immediately after WAN/Internet restore |
| Application / SQL Servers | 3 days after LAN/WAN restore |
| Reporting Servers | 5 days after LAN/WAN restore |

These RTO's should be considered best-case estimates. Bitfocus operates on a VMware virtual environment, with all server tiers fully virtualized. In the event of a disaster, the Disaster Assessment Team would assess the situation to determine if the local VM backups or the offsite VM backups (Amazon S3/Glacier) would be selected for recovery.

Once the assessment is complete, the Disaster Assessment Team will determine which temporary Data Center location to restore to. Current options are identified as Amazon Cloud or our Reno Data Center. Both locations are on standby.

# Recovery Point Objectives (RPO)

Recovery Point Objectives (RPO) reflects the estimated point in time to which recovery would be made based on current configurations and operations. the exact recovery point for each server will vary due to the time when the backup takes place and when the disaster occurs. Below are general guidelines for the different types of DR data protection.

| Data Protection Type | Recovery Point (Age of Data) |
|---|---|
| Onsite Backup | Up to 24 hours from disaster period. |
| Offsite Backup | Up to 7 days from disaster period. |

Customers who have purchased additional Disaster Recovery SLA plans may have shorter RPO.

# Roles of the Disaster Recovery Coordinator

The function of the Disaster Recovery Coordinator is vitally important to maintaining the plan in a consistent state of readiness. The Recovery Coordinator's role is multifaceted. Not only does the Coordinator assume a lead position in the ongoing life of the plan, but the Coordinator is a member of the Continuity Management Team in the event of a computer disaster.

The primary responsibilities of the Disaster Recovery Plan Coordinator are as follows:

- Distribution of the Disaster Recovery Plan
- Training the Disaster Recovery Teams
- Testing of the Disaster Recovery Plan
- Evaluation of the Disaster Recovery Plan Tests
- Review, change and update the Disaster Recovery Plan

In a disaster situation, the Disaster Recovery Plan Coordinator will:

- Facilitate communication between technical and non-technical staff
- Act as a Project Manager to coordinate the efforts of:
  - Technical Staff
  - Business Staff
  - Vendors
  - Other personnel as needed

The Disaster Recovery Coordinator for Bitfocus is Robert Herdzik. The alternate Disaster Recovery Plan Coordinator is Yanis Guenane.

# General Recovery Information

## Items Stored Offsite

1. Router / VPN Firmware and Export Settings.
2. A current copy of this disaster recovery plan.
3. A copy of Veeam Backup & Recovery 7 extract utility.
4. Weekly backups of full VMware Virtual Machine files of entire infrastructure and data.

All standard security and privacy precautions apply to offsite storage. The offsite storage facility is equipped with surge protectors and natural disaster protective measures.

Onsite backup includes all of the above, including nightly full Virtual Machine incremental backups of entire infrastructure and data.

## Server Recovery

These procedures outline the steps required to restore any Bitfocus servers. Recovery for the servers assume that:

- Good backup data exists and can be retrieved from either onsite or offsite storage
- Replacement servers are on standby or Amazon Cloud servers are on standby
- Network connectivity is established

A decision must be made as to where the recovery will take place (Amazon Cloud or Reno Data Center). This decision is not made ahead of time since the specifics of the incident requiring recovery is not known.

# Disaster Recovery Plan Maintenance

The disaster recovery plan is a "living" document. Failure to keep it current could severely impact Bitfocus' ability to successfully recover in the event of a disaster.

Some information contain in the plan is more dynamic than other information. A matrix of events and recommended maintenance schedule is included in this section. It is important to document changes to the plan and ensure that all copies of the plan are updated.

Changes to the plan could occur more frequently than the time frames listed in the following table. Major hardware upgrades might affect business recovery contracts as well as this plan. Software changes, personnel changes and other changes that affect the plan should be updated as soon as possible, not just when the recommended intervals occur.

| Period | Action |
|---|---|
| Quarterly | Review all job changes and update plan with new personnel assignments |
| | Have any new application servers been implemented? If so, have all disaster recovery implication been addressed? |
| | Have there been any major changes to existing applications? If so, update the recovery plan accordingly |
| | Has the hardware configuration changed? If the changes affect your ability to recover, make appropriate changes to the recovery configuration |
| | Update the Network Configuration Diagrams / Infrastructure Wiki |
| | Visit the off-site storage location and ensure documentation is available and current |
| | Ensure all team assignments are still valid |
| Semiannually | Test the plan and update it based on the results of the test |
| Annually | Review Amazon / Azure retention requirements |
| | Review Insurance coverage |

## Testing the Disaster Recovery Plan

The Disaster Recovery Coordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. On an on-going basis this frequency appears to be adequate considering the systems involved. However, special tests are to be given consideration whether there has been a major revision to the plan or significant changes in the software, hardware or data communications have occurred.

The objectives of testing the disaster recovery plan are as follows:

- Simulate the conditions of an ACTUAL Business Recovery situation.
- Determine the feasibility of the recovery process.
- Identify deficiencies in the existing procedures.
- Test the completeness of the business recovery information stored at the Offsite Storage Location.
- Train members of the disaster recovery teams.

The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the disaster recovery plan's acceptance. Subsequent tests should be to the extent determined by the Disaster Recovery Coordinator that are cost effective and meet the benefits and objectives desired.

## Sample Recovery Test Agenda

1. What is the purpose of the test?
2. What are the test objectives?
3. How will the successful achievement of these objectives be measured?
4. At the conclusion of the test, collect test measurements from all participants.
5. Evaluate the test results. Determine if the test was successful or not.
6. Determine the implications of the test results. Does success for this test imply success in all recovery scenarios?
7. Update the plan based on results of the test.

# HMIS
# Data Quality Plan

Cleveland/Cuyahoga County Continuum of Care

## HMIS Data Quality Plan

### 1.1 *Introduction*

This document describes the Homeless Management Information System (HMIS) data quality plan for the Cleveland/Cuyahoga County Continuum of Care (CoC). This document includes data quality standards and Protocols for ongoing data quality monitoring which meet the requirements outlined in the latest version of the Department of Housing and Urban Development (HUD) Data Standards. This HMIS Data Quality Plan shall be updated annually, and shall include the latest HMIS data standards set by HUD and Cleveland/Cuyahoga County CoC.

### 1.2 *HMIS Data and Technical Standards*

HMIS is a locally administered electronic data collection tool used to collect ongoing longitudinal data on homeless or at-risk families and individuals who receive assistance from local homeless service providers. Data collected can be used to evaluate the extent and nature of homelessness in our community. Information obtained from the system will assist with identification of client needs and service delivery.

In July 2003, the Department of Housing and Urban Development (HUD) published a draft notice of the HMIS Technical Data Standards. In July 2004, HUD finalized and published the HMIS Technical Data Standards in the Federal Register. HUD's objective was to encourage communities around the nation to set up an HMIS. The notice specified which data elements should be collected in order to ensure consistency across the nation and establish minimum baseline policies and procedures for privacy, confidentiality and security standards designed to protect client level data. In 2010, HUD amended and released the HMIS Technical Data Standards.

Cuyahoga County has adopted the use of *Clarity* (from Bitfocus Inc.) as its HMIS software solution. *Clarity* is a web-based application that requires no local software installation. It provides automatic reports to meet HUD reporting requirements and offers flexibility so that local agencies can customize its use for local needs. This platform was selected by a group of representatives of the local Continuum of Care in 2020, following a highly participatory process of analysis of system needs and comparative examination of several top-rated software platforms.

The Homeless Management Information System (HMIS) project is administrated by the Cleveland/Cuyahoga County Office of Homeless Services. The project utilizes the Internet-based technology to assist homeless service organizations across Cuyahoga County to capture information about the clients that they serve.

### 1.3 *What is Data Quality?*

Data Quality is the term that refers to the reliability, validity, and comprehensiveness of client-level data collected in HMIS. Good data quality represents reliable and valid data on persons accessing the homeless assistance system. With a strong data quality plan, multiple reports such as HUD Annual Performance Report (APR), Longitudinal System Analysis Report (LSA), and the Systems Performance Measure Report (SPMs) will be more accurate, and the HMIS coordinator will spend less time fixing errors. There are four main components to establish good data

quality: timeliness, completeness, accuracy, and consistency. Data Quality Standards are established, monitored, and updated annually by the HMIS Lead Agency.

### 1.4 *What is a Data Quality Plan?*

A data quality plan is a community-level document that facilitates the ability of the CoC to achieve statistically valid and reliable data. The data quality plan's purpose is to standardize and communicate expectations, and to provide guidance and support for all participating agencies. A data quality plan is generally developed by the Continuum of Care and the HMIS Lead Agency with input from community stakeholders and is formally adopted by the CoC. In short, a data quality plan sets expectations for agencies that use HMIS to capture reliable and valid data on persons accessing the homeless assistance system.

### 1.5 *What is a Data Quality Monitoring Plan?*

A data quality monitoring plan is a set of procedures which outline a regular, on-going process for analyzing and reporting on the reliability and validity of the data entered into HMIS at the project, program, and aggregate system levels. A data quality monitoring plan is the primary tool for tracking and generating information necessary to identify areas for data quality improvement.

## DATA QUALITY PLAN COMPONENTS

### 2.1 *Data Components*

It is important that our community has the ability to understand the characteristics of the clients that are served. Service providers, community leaders and CoC leadership need to be able to articulate the impact of our efforts. To ensure that this is possible, agencies must use both the Universal Data Set and the Program Specific Data Set. Coordinated Intake is responsible for collecting the initial, complete data set for each individual and household member entered into HMIS. All Emergency Shelters, Transitional Housing, Safe Havens, RRH and Permanent Supportive Housing projects should review, update and enter new information relative to the required set of data elements. All overflow and outreach projects should collect, at a minimum, the Universal Data Set. While CI is primarily responsible for the entry of the initial data set for all clients and household members, there are exceptions where an ES, TH, SH, RRH, or PSH project may have to assume that role.

Data quality evaluations will be based on the timeliness, completeness and accurate collection of the appropriate data set for each respective program. Failure to comply with the data standards described below will be addressed on a case-by-case basis.

### 2.2 *Data Timeliness*

The implementation of Coordinated Intake & Assessment has created the necessity for timely data entry. Timely data collection ensures that each client receives appropriate referrals and access to services. Each Participating Agency End User will rely on the Coordinated Intake Packet and the Universal Intake form for complete information (project referrals, entry dates, etc.) for each individual or member of a household. This information will subsequently be entered into HMIS and used to manage and track service delivery. Each Participating Agency will strive for real-time, or close to real-time, data entry. This is defined by either immediate data entry upon the client receiving an assessment or within one business day of the client assessment.

- Coordinated Intake and Assessment: Universal Data, Program Specific Elements, Entry, Service Transaction of Case Management, Referrals to CoC Providers and Exit must be entered within **1 business day**.

- Emergency Shelters: Universal Data, Program Specific Elements, Entry, Service Transaction of Emergency Shelter and Exit must be entered within **2 business days**.

- Transitional Housing Projects: Universal Data Elements, Program Specific Data Elements, Entry, Service Transaction of Transitional Housing and Exit must be reviewed and updated within **1 business day**.

- Permanent Supportive Housing Projects: Universal Data Elements, Program-Specific Data Elements, Entry, Service Transaction of Permanent Supportive Housing and Exit must be reviewed and updated within **1 business day**.

- Prevention & Rapid Re-housing Projects: Universal Data Elements, Program-Specific Data Elements, Entry, the initial Service Transaction of Case Management must be entered within **2 business days**.

- Outreach Projects: Limited data elements must be entered within **2 business days** of the first outreach encounter. Upon engagement for services, all remaining Universal Data Elements must be entered within **5 business days**.

- Supportive Services Only Projects: Universal Data Elements, Program Specific Data Elements, Entry, Service Transaction (provider quicklist) and Exit must be entered within **2 business days**.

***Clients entered into the HMIS via a data integration process will not follow the above deadlines and instead enter into HMIS in accordance with guidelines setup with each individual data integration project.***

**Agency Self-Assessment Procedure:**

**Data Entry Timeliness Reports** –It is important that agencies be able to measure the timeliness of their data entry. The [HUDX-225] HMIS Data Quality Report will help identify any short-comings associated with meeting the data entry objective. Each agency must run this report on a monthly basis to evaluate the timeliness of data entry. Additionally, agencies should also run the [HUDX-227] Annual Performance Report monthly to assist in identifying further data quality issues. (Agencies who do not meet the timeliness requirement should work with the System Administrator and begin running this report on a weekly basis until they have corrected any issues.) Agencies should run a each report for each project type, and a written corrective action plan should be put in place to address any issues that are not in accordance with the data timeliness requirements. A copy of the written corrective action plan should be e-mailed to HMIS System Administrator.

**2.3** ***Data Completeness***

All data entered into HMIS shall be complete. Partial or missing data can negatively affect our ability to provide appropriate and accurate referrals and services. It is every End User's responsibility to report a complete picture of persons served for each project within their agency.

The goal is always to collect 100% of the data elements for all individuals and members of a household. This is not always realistic or possible. Therefore, an acceptable range of null/missing and unknown/don't know/refused responses has been established, depending on the data element and the project type. Missing data elements are data elements that were either not collected or collected but were not entered into HMIS. Don't know/Refused data elements are those data elements that were not collected because the client either doesn't remember the information or refuses to answer the question. Don't know/Refused is from the clients' perspective and is not used to denote that the information is null or void.

Participating agencies will make their best effort to record accurate data. Only when a client refuses to provide his or her or dependent's personal information and the project funder does not prohibit it, it is permissible to enter incomplete client data. Some recommended procedures to follow are:

- If a client will not provide their date of birth, you may collect the age and set the date of birth to 1/1/XXXX, where XXXX is the actual birth year.

- If a client refuses to provide the identifiable elements, record the answer as "refused".

If a client's record already exists in HMIS, the agency must not create a new alias record. Participating Agencies should always use the Unique ID under which Coordinated Intake issued the project referral. The Participating Agency is responsible for any duplication of services that results from creating a duplicate client record or using the incorrect Unique ID.

All project types are strongly encouraged to achieve 100% compliance with all data quality standards. If 100% accuracy is not possible after multiple attempts at obtaining the required data, the following acceptable ranges apply:

Coordinated Intake and Assessment: **95%**
Emergency Shelters (project – reserved bed): **overall 95%**
Emergency Shelters (overflow – night to night entry, no reserved bed): **overall 85%**
Transitional and Permanent Supportive Housing Projects: **overall 95%**
ESG Rapid Re-Housing: **overall 95%**
Outreach Projects: **overall 75%**
Supportive Services Only Projects: **overall 95%**

**Acceptable range of missing (null) and unknown (don't know / refused) responses by project type:**

| | TH, PSH, SSO, ESG, Emergency Shelter, Federal | | Emergency Shelter (overflow) | | Outreach | |
|---|---|---|---|---|---|---|
| **Data Element** | **Missi** | **Don't** | **Missi** | **Don't** | **Missi** | **Don't** |
| **First & Last Name** | 0% | 2.5% | 0% | 2.5% | 0% | 2.5% |
| **Full SSN** | 0% | 2.5% | N/A | N/A | N/A | N/A |
| **Date of Birth (DOB)*** | 0% | 2.5% | 0% | 2.5% | 0% | 2.5% |
| **Race** | 0% | 2.5% | 0% | 2.5% | 0% | 2.5% |
| **Ethnicity** | 0% | 2.5% | 0% | 2.5% | 0% | 2.5% |
| **Gender** | 0% | 2.5% | 0% | 2.5% | 0% | 2.5% |
| **Veteran Status** | 0% | 2.5% | 0% | 2.5% | 0% | 10% |
| **Disabling Condition** | 0% | 2.5% | 0% | 10% | 0% | 10% |
| **Residence Prior to Proiect Entrv** | 0% | 2.5% | 0% | 10% | 10% | 10% |
| **Project Entry Date** | 0% | N/A | 0% | N/A | 0% | N/A |
| **Proiect Exit Date** | 0% | N/A | 0% | N/A | 0% | N/A |
| **Destination** | 0% | 2.5% | 0% | 10% | 0% | N/A |
| **Relationship to Head of Household** | 0% | 2.5% | 0% | 2.5% | 0% | 5% |
| **Client Location** | 0% | 2.5% | 0% | 2.5% | 0% | 2.5% |
| **Length of Time on Street, in ES or SH** | 0% | 2.5% | 0% | 10% | 0% | 10% |
| **Zip Code of Last Permanent Address** | 0% | 2.5% | 0% | N/A | N/A | N/A |
| **Housing Status** | 0% | 2.5% | 0% | 2.5% | 0% | 2.5% |
| **Income & Sources** | 0% | 2.5% | N/A | N/A | N/A | N/A |
| **Non-Cash Benefits** | 0% | 2.5% | N/A | N/A | N/A | N/A |
| **Health Insurance** | 0% | 2.5% | N/A | N/A | N/A | N/A |
| **Domestic Violence** | 0% | 2.5% | N/A | N/A | N/A | N/A |
| **Disability Type(s)** | 0% | 2.5% | 0% | 10% | 0% | 10% |
| **Addt'l PDE's as req'd by Federal Partners** | 0% | 2.5% | N/A | N/A | N/A | N/A |

*Date of Birth (DOB) – if client is not aware of their DOB use their age to calculate the year and enter the DOB in as 01/01/XXXX (which denotes the year associated with the age). Quality of DOB filed should be listed as "Client refused".
**The completeness requirement applies to each of the questions in the category.

**The Office of Homeless Services will utilize the data completeness standards in the chart above as we collect and review baseline data for HMIS Data Quality Completeness for the CoC. We will examine the findings and amend the above standards as appropriate.**

**Agency Self-Assessment Procedure:**
**Data Completion Scores –** Using the appropriate DQ reports ([HUDX-225] HMIS Data Quality Report & [HUDX-227] Annual Performance Report) all agencies should evaluate if all client level

data that is entered into HMIS adheres to appropriate project type completeness score. These reports must be generated and evaluated by the agency on a monthly basis. (Agencies who do not meet the timeliness requirement should begin running this report on a weekly basis versus a monthly basis until they have corrected any issues.) Corrective action should be taken if necessary to ensure that the agency meets or exceeds the goal for the appropriate project type. Should an agency fall short for the data completeness requirements, a written corrective action plan must be submitted to the HMIS System Administrator via email.

### 2.4 *Bed/Unit Utilization Rates and or Service Volume Rate*

One of the primary features of an HMIS is the ability to record the number of client stays or bed nights at a homeless residential facility. In HMIS, project beds or units are reflected within the Bed Inventory section of each appropriate Provider Profile. HMIS End Users for each emergency shelter, transitional housing and permanent supportive housing facility will enter a project entry for the client into HMIS at the time a bed or unit assignment is made. The client's project entry remains open in HMIS until he or she exits the project. When the client exits the project, they are considered exited from the bed or unit.

| Project Type | Target Utilization Rate | Acceptable Utilization |
|---|---|---|
| Emergency Shelter | 100% | 75% - 105% |
| Transitional Housing | 100% | 80% - 105% |
| Permanent Housing | 100% | 85% - 105% |

### 2.5 *Data Accuracy & Consistency*

Data accuracy can be a challenge in regards to HMIS. The level of accuracy relies on the client's ability to provide the correct information and the intake worker's ability to document and enter the data accurately. Data must also be collected in a consistent matter in order to ensure accuracy (i.e. Universal Intake Form, Outstanding Referral Report).

Accuracy will be assessed through monitoring activities outlined in the Data Quality Plan. Information entered into HMIS must be valid and accurately represent information on persons served for each Participating Agency. Inaccurate information is worse than incomplete information. It is better to answer "don't know or "refused" than to enter inaccurate information. To ensure the most up-to-date and complete data, data entry errors must be addressed either weekly or as they are detected.

All data entered into HMIS is provided by the client, as documented by the intake worker or by the program case manager. Data entered must meet a 100% accuracy rate. Recording inaccurate information is strictly prohibited, unless in cases when a client refuses to provide correct personal information (see below). All data in HMIS shall be collected and entered in a common and consistent manner across all projects. To that end, all End Users and their respective Supervisors will complete an initial training before accessing the live HMIS system.

**Agency Self-Assessment Procedure:**

- **Data Accuracy:** Agencies are ultimately responsible for the accuracy of their data. In order to ensure accuracy, source documentation must be reviewed on a consistent basis. The System Administrator will work with Coordinated Intake staff to review and update source documentation at the time of initial assessment. This form will be

distributed to all Participating Agencies. It is each agency's responsibility to develop a self-monitoring plan to evaluate/audit the accuracy of their data entered into HMIS. Agencies must designate agency personnel (HMIS Site/Agency Administrator) to perform monthly accuracy audits. The HMIS Site/Agency Administrator is responsible for ensuring that accuracy of data entered into HMIS by sampling the data. They can use the following methods:

Sampling: A sampling of client source documentation can be performed to measure the data accuracy rate. Agencies will be required to self-audit 10% of their client records for each program and project on a monthly/quarterly basis, comparing the source information to that entered in HMIS. The agency audit form should be completed and kept for the HMIS Lead Agency staff's annual review.

Data Consistency Checks: The HMIS Site/Agency Administrator should check data accuracy and consistency by running DQ reports to analyze the completion of project entry records, issuing of service transactions, interim reviews/recertifications and exits. For example, the following instances will be flagged and reported as errors:

- Mismatch between exit/entry data
- Conflicting elements within the assessments
- Household composition error

## DATA QUALITY MONITORING

### 3.1 *Roles and Responsibilities*

- Agency – Each Participating Agency's Executive Director and/or Program Manager must designate an agency representative to act as the agency's HMIS Site/Agency Administrator. It is the responsibility of the Executive Director and HMIS Site/Agency Administrator to ensure compliance with the policies and procedures of this manual. Participating Agencies are ultimately responsible for the quality of their data. If agencies abide by the policies and procedures outlined in the Policy and Procedure Manual and monitor the integrity and security of client data, it will ensure that they perform well in an audit. Agencies will be held responsible for the security of their client's data and will be held accountable for the liability for any misuse of the software by agency staff. Performing the monthly review of data outlined in this manual will ensure that agencies are aware of their Data Quality performance. It is the responsibility of the HMIS Lead Agency to coordinate and conduct the annual site visit for each agency. Each Participating Agency will make available 10% of client records for each project available (randomly selected records).

- HMIS Lead Agency – The Office of Homeless Services will notify the Participating Agency 7 days in advance of a site visit and will conduct the site visit in a professional, consistent and fair manner. Provide guidance to increase the understanding and definition of federal policies, procedures, guidelines and best practices. Provide oversight/monitoring of CoC Data Quality and Security standards.

### 3.2 *Monitoring Frequency*

- Data Timeliness, Data Completeness and Data Accuracy: monthly review by agency; monthly submission of APR to HMIS System Administrator and subsequent feedback from HMIS Sys Admin.

- Program Audit: annual audit by HMIS Lead Agency

- Other: Data quality monitoring may be performed outside the regularly scheduled reviews, if requested by program funders or other interested parties (the agency itself, HMIS Lead Agency, CoC, HUD, or other Federal and local government agencies)

**3.3 *Compliance***

- Data Timeliness: The average timeliness rate in any given month should be within the allowed timeframe.

- Data Completeness: there should be no missing (null) data for required data elements. Responses that fall under unknown (don't know or refused) should not exceed the allowed percentages in any given month (see Data Completeness section for standards). Housing providers should stay within the allowed utilization rates.

- Data Accuracy: The percentage of client files with inaccurate HMIS data should not exceed 10%. (For example, if the sampling includes 10 client files, then 9 out of 10 of these files must have the entire set of corresponding data entered correctly in HMIS.)

**3.4 *Data Quality Reporting and Outcomes***

The HMIS System Administrator will receive updated APRs from Agency Administrators once a month for the previous month. The HMIS System Adminstrator will evaluate data quality monthly and ensure that agencies that fall below the proposed standards are notified of any deficiencies. Notifications will include any findings and recommended corrective actions. Overall, the HMIS Lead Agency Staff will be aware of each Participating Agency's performance. Any patterns of error will be reported to the respective Agency Executive Director for corrective action.

- Participating agencies are expected to correct data errors as soon as identified or within maximum of 7 days of notification. Data quality issues that have not been addressed for consecutive months will be brought to the attention of the Director of the Office of Homeless Services (OHS). If after the next quarter there has been insufficient improvement, it will be reported to CoC Advisory Board.

- Projects will be considered to be out of compliance with their contract agreements if they do not demonstrate a good faith effort to make necessary data corrections after consecutive months of data quality that does not meet the standards outlined in this manual.

| DE | Element | Collection Points | | | | | | Required Metadata Elements | |
|---|---|---|---|---|---|---|---|---|---|
| | | Record Creation | Project Start | Update/ Occurrence Point | Annual Assess-ment | Project Exit | Post-Exit | Enrollment ID | Data Collection Stage |
| 3.01 | Name | X | | | | | | | |
| 3.02 | Social Security Number | X | | | | | | | |
| 3.03 | Date of Birth | X | | | | | | | |
| 3.04 | Race | X | | | | | | | |
| 3.05 | Ethnicity | X | | | | | | | |
| 3.06 | Gender | X | | | | | | | |
| 3.07 | Veteran Status | X | | | | | | | |
| 3.08 | Disabling Condition | | X | | | | | X | |
| 3.1 | Project Start Date | | X | | | | | X | |
| 3.11 | Project Exit Date | | | | | X | | X | |
| 3.12 | Destination | | | | | X | | X | |
| 3.15 | Relationship to Head of Household | | X | | | | | X | |
| 3.16 | Client Location | | X | X | | | | X | X |
| 3.2 | Housing Move-In Date | | | X (0…1) | | | | X | |
| 3.917 | Prior Living Situation (A) and (B) | | X | | | | | X | |
| 4.02 | Income and Sources | | X | X | X | X | | X | X |
| 4.03 | Non-Cash Benefits | | X | X | X | X | | X | X |
| 4.04 | Health Insurance | | X | X | X | X | | X | X |
| 4.05 | Physical Disability | | X | X | | X | | X | X |
| 4.06 | Developmental Disability | | X | X | | X | | X | X |
| 4.07 | Chronic Health Condition | | X | X | | X | | X | X |
| 4.08 | HIV/AIDS | | X | X | | X | | X | X |
| 4.09 | Mental Health Disorder | | X | X | | X | | X | X |
| 4.1 | Substance Use Disorder | | X | X | | X | | X | X |
| 4.11 | Domestic Violence | | X | X | | | | X | X |
| 4.12 | Current Living Situation | | | X | | | | X | |
| 4.13 | Date of Engagement | | | X (0…1) | | | | X | |
| 4.14 | Bed-Night Date | | | X | | | | X | |
| 4.19 | Coordinated Entry Assessment | | | X | | | | X | |
| 4.2 | Coordinated Entry Event | | | X | | | | X | |
| W1 | Services Provided - HOPWA | | | X | | | | X | |
| W2 | Financial Assistance - HOPWA | | | X | | | | X | |
| W3 | Medical Assistance | | X | X | | X | | X | X |
| W4 | T-cell (CD4) and Viral Load | | X | X | X | X | | X | X |
| W5 | Housing Assessment at Exit | | | | | X | | X | |
| W6 | Prescribed Anti-Retroviral | | X | X | | X | | X | |
| C1 | Well-being | | X | | X | X | | X | X |
| C2 | Moving On | | | X | | | | X | |
| C3 | Youth Education Status | | X | | | X | | X | X |
| P1 | Services Provided-PATH Funded | | | **X** | | | | **X** | |
| P2 | Referrals Provided - PATH | | | **X** | | | | **X** | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| P3 | PATH Status | | | X (0…1) | | | | X | |
| P4 | Connection with SOAR | | X | X | X | X | | X | X |
| R1 | Referral Source | | X | | | | | X | |
| R2 | RHY-BCP Status | | X | X (0…1) | | | | X | |
| R3 | Sexual Orientation | | X | | | | | X | |
| R4 | Last Grade Completed | | X | | | X | | X | X |
| R5 | School Status | | X | | | X | | X | X |
| R6 | Employment Status | | X | | | X | | X | X |
| R7 | General Health Status | | X | | | X | | X | X |
| R8 | Dental Health Status | | X | | | X | | X | X |
| R9 | Mental Health Status | | X | | | X | | X | X |
| R10 | Pregnancy Status | | X | X | | | | X | X |
| R11 | Formerly a Ward of Child Welfare or Foster Care Agency | | X | | | | | X | |
| R12 | Formerly a Ward of Juvenile Justice System | | X | | | | | X | |
| R13 | Family Issues | | X | | | | | X | |
| R14 | RHY Service Connections | | | X | | | | X | |
| R15 | Commercial Sexual Exploitation | | | | | X | | X | |
| R16 | Labor Exploitation | | | | | X | | X | |
| R17 | Project Completion Status | | | | | X | | X | |
| R18 | Counseling | | | | | X | | X | |
| R19 | Safe and Appropriate Exit | | | | | X | | X | |
| R20 | Aftercare Plans | | | | | | X | X | |
| U1 | Worst Housing Situation | | X | | | | | X | |
| V1 | Veteran's Information | X | | | | | | X | |
| V2 | Services Provided - SSVF | | | X | | | | X | |
| V3 | Financial Assistance - SSVF | | | X | | | | X | |
| V4 | Percent of AMI (SSVF Eligibility) | | X | | | | | X | |
| V5 | Last Permanent Address | | X | | | | | X | |
| V6 | VAMC Station Number | | X | | | | | X | |
| V7 | HP Targeting Criteria | | X | | | | | X | |
| V8 | HUD-VASH Voucher Tracking | | X | X | | X | | X | X |
| V9 | HUD-VASH Exit Information | | | | | X | | X | |