communityshelterboard

FY23 HMIS Policies & Procedures

Updated: March 2023

TABLE OF CONTENTS

1. Introduction

1.1 Community Shelter Board

VISION

Everyone has a place to call home.

MISSION

Community Shelter Board leads a coordinated, community effort to make sure everyone has a place to call home. CSB is the collective impact organization driving strategy, accountability, collaboration, and resources to achieve the best outcomes for people facing homelessness in Columbus and Franklin County.

1.2 Project Summary

The Homeless Management Information System (HMIS) is used to collect, monitor, and evaluate homeless and housing services in Columbus and Franklin County. Currently, over 340 users in 16 agencies are using HMIS to collect data for over 90 homeless and housing related programs throughout Franklin County. The HMIS project is supported by CSB through a Data and Evaluation Department staffed by a full time CSB Database Administrator, Senior Data Analyst, Data Analyst, Data and Grants Coordinator, and Associate Director.

HUD requires each local CoC to have an HMIS that complies with the HUD standards, is used by all HUD funded entities in the continuum and is able to produce aggregate reporting at system and community level. Prior to 2008, CSB's HMIS did not fully comply with these standards, which led to the need to upgrade the system.

The HMIS Selection Committee recommended on September 11, 2007 to start contract negotiations with Bowman Systems (now Wellsky) as the vendor for the upgraded HMIS, ServicePoint. The recommendation was presented and adopted by the CoC Steering Committee on October 9, 2007. Implementation of the new system was started in November 2007. The implementation due date and "go live" date was July 14, 2008.

Due to an outdated ServicePoint system in an increasingly data-driven environment, CSB decided to seek a new HMIS vendor through an RFP process in January 2021. After narrowing the submission to 3 vendors and gathering feedback from select partner agencies, CSB made the decision to start contract negotiations with BitFocus as the vendor for the new HMIS, Clarity. The system migration process started in early February 2021, with a "go live" date of July 1, 2021.

1.3 Governing Principles

The goal of HMIS is to support the delivery of homeless and housing services in Columbus and Franklin County. HMIS is:

- a benefit to individual clients through enhanced service delivery
- a tool for the provider agencies in managing programs and services
- a guide for CSB and its funders regarding community resource needs and service delivery

While accomplishing these goals, CSB recognizes the primacy of client needs in the design and management of HMIS. These needs include both the need continually to improve the quality of homeless and housing services in Columbus and Franklin County, and the need vigilantly to maintain client confidentiality, treating the personal data of our most vulnerable populations with respect and care. As the guardians entrusted with this personal data, we have both a moral and a legal obligation to ensure that this data is being collected, accessed and used appropriately. The needs of the people we serve are the driving forces behind HMIS.

With this in mind, HMIS will also be:

- a **confidential and secure environment** protecting the collection and use of client data.

CSB will follow, at all times, the Privacy and Data Security Policy as posted on CSB's website at csb.org.

1.4 Terminology

Definitions of some of the terms used in this manual are as follows:

Authentication: The process of identifying a user in order to grant access to a system or resource. Usually based on a username and password.

BitFocus: The company who developed the software used for Clarity HMIS.

Clarity HMIS : The specific HMIS utilized in Columbus, Ohio.
A software package developed by BitFocus which tracks data about people in housing crisis in order to determine individual needs and provide aggregate data for reporting and planning. This software is web-based and uses a standard web browser to access the database.

Contributing HMIS Organization (CHO): Any agency, organization or group who has signed a Partnership Agreement or an HMIS Agreement ("Agreement") with CSB and is allowed access and contributes data to the HMIS database. These agencies connect independently to the database via an internet web browser.

Continuum of Care Project: Project receiving funding from the US Department of Housing and Urban Development through the competitive Continuum of Care application process.

CSB: Community Shelter Board. CSB is an intermediary funding and planning organization in Columbus, Ohio, with the goal of eliminating homelessness in Columbus and Franklin County.

CSB Database Administrator: The job title of the person at CSB who is the System Administrator for HMIS.

Database: An electronic system for organizing data so it can easily be searched and retrieved. Usually organized by fields and records.

Encryption: Translation of data from plain text to a complex code. Only those with the ability to unencrypt the encrypted data can read the data. Provides security.

Firewall: A method of controlling access to a private network, to provide security of data. Firewalls can use software, hardware, or a combination of both to control access.

Partner Agency: Agencies receiving funding from Community Shelter Board.

Server: A computer on a network that manages resources for use by other computers in the network. For example, a file server stores files that other computers (with appropriate permissions) can access. One file server can "serve" many files to many client computers. A database server stores a data file and performs database queries for client computers.

Agency Administrator: The person responsible for system administration at the agency level. Responsible for basic trouble-shooting, quality assurance of data and organizational contact with the CSB Database Administrator.

System Administrator: The person with the highest level of user access in HMIS. This user has full access to all user and administrative functions.

User: An individual who uses a particular software package; in this case, the HMIS software.

User License: An agreement with a software company that allows an individual to use the product. In the case of HMIS, user licenses are agreements between CSB and BitFocus that govern individual connections to HMIS.

1.5 Ownership

HMIS, and any and all data stored in HMIS, is the property of the Community Shelter Board. CSB has final control over the creation, maintenance and security of HMIS. In order to ensure the integrity and security of sensitive client confidential information and other data maintained in the database, CSB will require all CHOs to sign an agreement ("Agreement") prior to being given access to HMIS. The Agreement includes terms regarding the confidentiality of client information, duration of access, an acknowledgement of receipt of the Policies and Procedures Manual, and an agreement to abide by policies and procedures related to HMIS, including all security provisions contained therein.

Violations of the Agreement, including without limitation the failure to comply with the policies and procedures related to HMIS, may subject the CHO to discipline and termination of access to HMIS and/or to termination of other CSB contracts.

2. Implementation Overview

2.1 Relationship to CHOs

Contributing HMIS Organizations (CHOs) are those agencies allowed by CSB to connect to HMIS for the purposes of data entry, data editing and data reporting. These agencies are CSB Partner Agencies and Other Agencies. Partner Agencies are agencies receiving funding directly and/or pass-through from Community Shelter Board. Other Agencies choose to participate in the HMIS though they do not receive funding from Community Shelter Board.

Relationships between CSB and CHOs are governed by any standing agency-specific agreements already in place (such as the Partnership and Master Provider Agreements), the HMIS Agency Agreement, and the contents of the Policies and Procedures Manual, the HMIS Data Reference and Dictionary, and the CSB Privacy and Data Security Policy as found on CSB's website at csb.org, and updated from time to time. Update to those documents will be communicated to CHOs in a timely manner. All CHOs, regardless of type, are required to abide by the policies and procedures outlined in this manual.

2.2 Relationship to BitFocus

CSB contracts with BitFocus on an annual basis. Through this contract, BitFocus provides software maintenance, application support, and database maintenance and hosting. CSB has purchased software and user licenses, for an annual fee, to be used to access HMIS. CSB is responsible for maintaining the HMIS contract with BitFocus, and the CSB Database Administrator is the designated contact to BitFocus. The CSB Database Administrator is responsible for providing the main conduit for communications between CHOs and BitFocus in order to provide coherent and timely information exchange.

While most communications with BitFocus related to HMIS will be channeled through the CSB Database Administrator, CHOs may choose to contract independently with BitFocus to acquire further database customization or other services not related to HMIS. In such cases, the individual agency is solely responsible for negotiation of, and payment for, these services, as well as all communication with BitFocus regarding these matters.

2.3 Central Server

Clarity HMIS is hosted on BitFocus servers. The BitFocus network is protected by strong firewalls, and all traffic is logged and monitored by System Administrators. All data is backed up using a combination of overlapping backup strategies.

HMIS grants access only to authorized users by utilizing username and password authentication. HMIS webpages are served over the HTTPS (Secure HTTP) protocol (SSL) and uses 2048-bit encryption or better. HMIS also includes multiple security levels to control the amount of access a valid user can have.

2.4 Security Infrastructure

CSB, by paying a monthly fee, is taking advantage of BitFocus's maintenance and hosting services for HMIS. BitFocus employs a full-time staff of experts dedicated to keeping their clients up, running and secure, using the latest technology. This technology includes physical security, firewalls, authentication through browser certificates, Windows secure server technology, and encryption of usernames, passwords, and all data passing to and from the database. It is the job of the CSB Database Administrator to maintain a point of contact between BitFocus and CSB and keep track of security issues at the central database.

Safeguards:

- Physically secure building with 24/7/365 staffing
- Biometric scanners
- Dual-factor authentication access
- Monitored security scanners

Technical Safeguards:

- Documented nightly backup and emergency recovery procedures
- Secure API capability with AES encrypted traffic
- Unique user authentication
- End-to-end data encryption with 2048 bit SSL encryption at rest and during transfer
- Role-based data access
- Automatic time-out and lockout
- Concurrent login prevention
- Two factor authentication
- IP whitelisting
- Automated audit logs

3. Roles and Responsibilities

3.1 Project Organization

Project Management

Policy: CSB is responsible for organization and management of HMIS.

Explanation: As the coordinating body for HMIS, Community Shelter Board is responsible for all system-wide policies, procedures, communication and coordination. CSB is the primary contact with BitFocus, and with its help, implements all necessary system-wide changes and updates.

CSB seeks to provide a uniform HMIS which yields the most consistent data for client management, agency reporting, and service planning. The primary position at CSB for HMIS management is the CSB Database Administrator. All system-wide questions and issues should be directed to the CSB Database Administrator. The Database Administrator reports to the CSB Associate Director. The Associate Director designates a Back-up Database Administrator. CSB's CEO, as head of the Community Shelter Board, is ultimately responsible for all final decisions regarding planning and implementation of HMIS.

Agency Administrators

Policy: Each CHO designates two Agency Administrators.

Explanation: The Agency Administrator is the primary HMIS contact at the agency. This person is responsible for:

- Providing a single point of communication between the CHO's end users and the CSB Database Administrator around HMIS issues
- Ensuring the stability of the agency connection to the Internet and HMIS, either directly or in communication with other technical professionals
- Training agency end-users
- Providing support for the generation of agency reports
- Managing agency user licenses
- Monitoring compliance with standards of client confidentiality and data collection, entry, and retrieval
- Participating in Agency Administrators training and regular meetings
- Participating as the advisors and consultants to the CSB Database Administrator

Designating two primary HMIS contacts and power-users at each agency increases the effectiveness of communication both between and within agencies.

Each CHO designates two Agency Administrators and sends each person's name and contact information to the CSB Database Administrator. Changes to that information should be promptly reported to the CSB Database Administrator. Agency Administrators receive additional training from the CSB Database Administrator.

User Access Levels

Policy: All HMIS Users have an appropriate level of access to HMIS data.

Explanation: HMIS allows multiple levels of user access to data contained in the database. Access is assigned when new users are added to the system and can be altered as needs change. For security purposes, appropriate access levels should be assigned to all users.

The CSB Database Administrator assigns appropriate user levels when adding new users. In the interest of client data security, the CSB Database Administrator will always attempt to assign the most restrictive access which allows efficient job performance.

CSB Communication with CHOs

Policy: The CSB Database Administrator is responsible for relevant and timely communication with each agency regarding HMIS.

Explanation: The CSB Database Administrator communicates system-wide changes and other relevant information to agencies as needed. The CSB Database Administrator also maintains a high level of availability to CHOs. While specific problem resolution may take longer, the CSB Database Administrator strives to respond to CHO questions and issues within one business day of receipt.

General communications from the CSB Database Administrator are directed towards the Agency Administrator, most of the time through email communication. Specific communications will be addressed to the person or people involved. The CSB Database Administrator is available via email or phone. The CSB website is used to distribute HMIS information. Agency Administrators are responsible for ensuring all their agency users are informed of appropriate HMIS related communications. Agency Administrators are also responsible for distributing that information to any additional people at their agency who may need to receive it, including, but not limited to, CEOs, client intake workers, and data entry specialists.

CHO Communications with CSB

Policy: CHOs are responsible for communicating needs and questions regarding HMIS directly to the CSB Database Administrator. The CHOs are encouraged to use a special email address, HMIS@csb.org, to submit support tickets.

Explanation: CHOs communicate needs and questions directly to the CSB Database Administrator. For HMIS support tickets, the CHO uses a special email address, HMIS@csb.org, to communicate issues with CSB. The Data and Evaluation team reviews the HMIS tickets and provides an initial response to the CHO within 24 hours.

Users at CHOs communicate needs, issues and questions to their Agency Administrator. If the Agency Administrator is unable to resolve the issue, the Agency Administrator contacts the CSB Database Administrator via email or phone, or HMIS support ticket. The goal of the CSB Database Administrator is to respond to CHO needs within one business day of the first contact.

System Availability

Policy: CSB and BitFocus provide a highly available database server and inform users in advance of any planned interruption in service.

Explanation: It is the intent of CSB and BitFocus that the HMIS database server will be available 24 hours a day, 7 days a week, 52 weeks a year to incoming connections. However, no computer system achieves 100% uptime. In the event of planned server downtime, the CSB Database Administrator informs agencies as much in advance as possible in order to allow CHOs to plan their access accordingly.

In the event that the database server is or will be unavailable due to disaster or routine maintenance, BitFocus contacts the CSB Database Administrator. The CSB Database Administrator contacts Agency Administrators and informs them of the cause and duration of the interruption in service. The CSB Database Administrator logs all downtime for purposes of system evaluation.

Ethical Data Use

Policy: Data contained in HMIS is used to support the delivery of homeless and housing services in Columbus and Franklin County. Each HMIS User affirms the principles of ethical data use and client confidentiality contained in the HMIS Policies and Procedures Manual and the HMIS User Agreement.

Explanation: CSB recognizes that the specific purpose for which the HMIS was created limits the uses of the data it contains to those which conform to this initial purpose. The data collected in HMIS is the personal information of people in the Columbus and Franklin County community who are experiencing a housing crisis. It is the responsibility of the guardians of that data to ensure that it is only used to the ends to which it was collected.

All HMIS users sign a HMIS User Agreement before being given access to HMIS. Any individual or CHO misusing, or attempting to misuse, HMIS data will be denied access to the database, and his/her/its relationship with CSB will be terminated.

CHO Grievances

Policy: CHOs contact the CSB Database Administrator to resolve HMIS problems.

Explanation: CSB is responsible for the operation of HMIS. Any problems with the operation or policies of HMIS are to be discussed with CSB. CSB has final decision-making authority over all aspects of HMIS.

CHOs bring HMIS problems to the attention of the CSB Database Administrator. If these problems cannot be resolved by the CSB Database Administrator, the CSB Database Administrator will take them to the CSB Associate Director, and finally to the CSB CEO. CSB's CEO shall have the final say in all matters regarding HMIS.

Client Grievance

Policy: Clients contact the CHO with which they have a grievance for resolution of HMIS problems. CHOs report all HMIS-related client grievances to CSB.

Explanation: Each agency is responsible for answering questions and complaints from their own clients regarding HMIS. CSB is responsible for the overall use of HMIS, and will respond if users or agencies fail to follow the terms of the Partnership or HMIS Agreements, breach client confidentiality, or misuse client data. Agencies are obligated to report all HMIS-related client problems and complaints to CSB, which will determine the need for further action.

Clients bring HMIS complaints directly to the agency with which they have a grievance. Agencies provide a copy of the HMIS Policies and Procedures Manual upon request, and respond to client issues. Agencies send copies of all client grievance forms recording HMIS-related client problems and complaints to the CSB Database Administrator. The CSB Database Administrator records all grievances and reports these complaints to the CSB Associate Director, who will take any necessary action. The CSB Database Administrator keeps a log of all complaints and concerns, and responds to individual complaints and patterns of concern with appropriate actions. These actions might include further investigation of incidents, clarification or review of policies, or sanctioning of users and agencies if users or agencies are found to have violated standards set forth in Agreements or the Policies and Procedures Manual.

CHO Hardware/Software Requirements

Policy: CHOs provide their own computer and method of connecting to Internet, and thus to HMIS.

Explanation: Because HMIS is a web-enabled software, all that is required to use the database is a computer, a valid username and password, and the ability to connect to the Internet by broadband or other high-speed connection. There is no unusual hardware or additional HMIS-related software installation required. BitFocus guidelines are:

MEMORY: 4 Gig recommended, (2 Gig minimum)
MONITOR: Screen Display - 1024 by 768 (XGA) or higher (1280x768 strongly advised)
PROCESSOR: Avoid using single-core CPUs
INTERNET CONNECTION: Broadband or other high-speed option
BROWSER: Mozilla Firefox or Google Chrome are recommended; Microsoft Edge and most other browsers are acceptable.

It is the responsibility of the CHO to provide a computer and connection to the Internet. If desired by the CHO, the CSB Database Administrator will provide advice as to the type of computer and connection.

CHO Technical Support Requirements

Policy: CHOs provide their own technical support for all hardware and software employed to connect to HMIS.

Explanation: The equipment used to connect to HMIS is the responsibility of the CHO.

Agencies provide internal technical support for the hardware, software and Internet connections necessary to connect to HMIS according to their own organizational needs.

HMIS Documentation Updates

Policy: CSB provides a HMIS Policies & Procedures Manual, QA Standards & Data Dictionary, and relevant forms and user guides for all HMIS Agency Administrators. These documents are kept up to date and in compliance with all HUD policies and requirements.

Explanation: The purpose of the HMIS policies and procedures is to provide Agency Administrators with guidance in maintaining compliance with HUD and Continuum of Care requirements and standards. They include information about how the software product is to be managed from an Agency Administrator perspective and the roles and responsibilities of an Agency Administrator and their CHO. CSB provides an electronic copy of the Policies and Procedures Manual containing procedures that are held in common for all CHOs.

A HMIS Agency Administrator manual provides information about how the software product is used in our community, contains procedures that are held in common for all CHOs, and includes common HMIS related forms. The QA Standards & Data Dictionary provides detailed information on the quality assurance standards and the data requirements for all programs and CHOs. CSB provides an electronic copy of the QA Standards & Data Dictionary for all CHOs. HMIS training videos provide specific technical instruction about how to use HMIS for both Agency Administrators and End Users.

The CSB Database Administrator updates all HMIS related forms and user guides annually, by the beginning of each new fiscal year. The HMIS documents are reviewed and kept up to date and in compliance with all HUD policies and requirements. In the event HUD issues changes to the requirements, affected policies and procedures and related documentation are reviewed and updated at that time as well. The updates are reviewed and approved by the CSB Associate Director. The updates are communicated and discussed with the HMIS Agency Administrators during the quarterly HMIS Administrator meetings. If HUD requirements necessitate immediate implementation of changes, this will be communicated to all Agency Administrators electronically, as soon as available. All documents will be available for download at www.csb.org.

3.2 Security

User Access

Policy: The CSB Database Administrator provides unique usernames and initial passwords to each agency user. Usernames are unique for each user and are comprised of the initial of the user's first name and the user's full last name, all lower case. Usernames and passwords may not be exchanged or shared with other users. The CSB Database Administrator has access to the list of usernames.

Explanation: Unique usernames and passwords are the most basic building block of data security. Not only is each username assigned a specific access level, but in order to provide to clients an accurate record of who has altered his or her record, when it was altered, and what the changes were, it is necessary to log a username with every change. Exchanging usernames seriously compromises security and accountability to clients.

The CSB Database Administrator provides unique usernames comprised of the user's first initial and full last name, all lower case, and initial passwords to each user upon completion of HMIS Certification, which includes basic security and privacy training. The sharing of usernames is considered a breach of the Agreement.

User Changes

Policy: The CHO Agency Administrator communicates any necessary changes to the role of CHO users. Only the CSB Database Administrator can change the roles of users within the HMIS.

Explanation: Only the CSB Database Administrator has the ability to add/delete user accounts and re-distribute user licenses to accommodate agency needs.

The Agency Administrator communicates any necessary changes to the list of agency users to the CSB Database Administrator. Changes in Agency Administrators must be reported to the CSB Database Administrator.

Passwords

Policy: Users have access to the HMIS via a username and password. Passwords reset every 90 days. Passwords must consist of at least 8 characters and include at least one digit. Users keep passwords confidential.

Explanation: Users have access to the CSB HMIS via a username and password. This method of access is unique to each user and confidential. Users are responsible for keeping their passwords confidential. For security reasons, passwords are automatically reset every 90 days.

The CSB Database Administrator issues a username and password to each new user who has completed training directed by the CHO. Every 90 days, passwords are reset automatically. On the 90th day, when the user logs in, the system requires the user to create a new password and enter it twice before accessing the database.

Password Recovery

Policy: All HMIS users can reset their own password via an automated email process. CSB's Database Administrator resets user passwords in the event there are issues with the automated process.

Explanation: In the event of a forgotten password, the HMIS End User resets that password, via an automated email process.

In the event of a forgotten password, the user whose password is forgotten resets their password through an automated email process by click on the "Forgot Password" link on the HMIS login page. The new password is valid from that time forward, until the next password expiration. In the event the automated process is not working, the user should reach out to their Agency Administrator, who will contact the CSB Database Administrator if needed.

Extracted Data

Policy: HMIS users maintain the security of any client data extracted from the database and stored locally, including all data used in custom reporting. HMIS users do not electronically transmit any unencrypted client data across a public network. CSB may initiate encrypted electronic communication via secure email.

Explanation: The report-writer function of HMIS allows client data to be downloaded to a file on the local computer, such that client data is left vulnerable, unless additional measures are taken. Such measures might include restricting access to the file by adding a password. For security reasons, unencrypted data may not be sent over a network that is open to the public. For example, while unencrypted data might be stored on a server and accessed by a client computer within the private local area network, the same unencrypted data may not be sent via email to a client computer not within the same local area network. CSB may initiate encrypted electronic communication via Microsoft secure email. Replies to these emails must be done through the Microsoft secure reply interface to maintain confidentiality of any sensitive information. HMIS users should apply the same standards of security to local files containing client data as to the HMIS database itself.

Data extracted from the database and stored locally is stored in a secure location and is not transmitted outside of the private local area network unless it is properly protected. Security questions are addressed with the CSB Database Administrator.

Data Access Location

Policy: Users ensure the confidentiality of client data, following all security policies in the HMIS Policies and Procedures Manual and adhering to the standards of ethical data use, regardless of the location of the connecting computer.

Explanation: Because HMIS is web-enabled software, users can connect to the database from locations other than the agency itself, using computers other than agency-owned computers. If such a connection is made, the highest levels of security must be applied, and client confidentiality must still be maintained.

All Policies and Procedures and security standards are enforced regardless of the location of the connecting computer.

Hardware & Software Security Measures

Policy: The Agency Administrator ensures all hardware and software used to access and/or store HMIS data is in a secure location where access is restricted to authorized staff. The Agency Administrator ensures all computers used to access and/or store HMIS data employ software security and access restriction measures.

Explanation: Because HMIS enables authorized users to download raw client-level data via the custom report writer to their hard drive or other electronic media, access to such computers and/or disks must be restricted to authorized personnel only.

The Agency Administrator ensures that any computers used to access HMIS and any disks used to store custom report information are located in a secure area where access is available to authorized personnel only. The Agency Administrator ensures that these same computers and disks utilize the following security measures listed below.

Computers:

- Locking screen savers
- Virus protection with auto update
- Individual network firewalls

Storage disks:

- Encryption
- Password protected

Multiple Log-on Restriction Policy

Policy: Individual HMIS users are not able to log on to HMIS from more than one workstation at a time, or able to access client level data (Protected Personal Information) from more than one location at a time.

Explanation: HMIS provides the ability to run reports *and download client-level data to local computer networks*. To ensure the security and accountability for such data, users must not be able to log on to more than one workstation at a time.

There are two acceptable scenarios for compliance:

1. When user logs on at the 2nd workstation, the system can provide a message notifying the user that they must first log off of the 1st workstation, or

2. When the user logs on at the 2nd workstation, the system can automatically log the user off of the 1st workstation and allow access at the 2nd workstation.

Remote Access Policy

Policy: HMIS is intended to be accessed on-site from the CHO's network, desktops, and laptops that are web capable.

The Remote Access Policy and Agreement is an extension of the User Agreement and HMIS Policies and Procedures manual. The user shall comply with all Policies, Procedures, Agreements and rules governing HMIS.

The Agency Administrator has the responsibility to assure the user is in compliance with this and all other Policies, Procedures, Agreements and rules governing HMIS.

All staff that access HMIS remotely must meet the standards detailed in the System Security policies and procedures (see Policy and Procedures) and may only access it for activities directly related to their job.

Examples of Remote Access:

1. CHO offices on secure networks to support agency use of the system.
2. Training Centers on secure networks when providing services or training in the field.
3. Private Home Office on secure networks to provide client assistance and real-time data entry of client data.

Explanation: Because HMIS enables authorized users to access client-level data via the internet on web-capable devices, remote access must be executed carefully.

Requirements for Remote Access of HMIS include:

- Remote access will only be allowed on secure networks. User will not access HMIS on any unprotected, free, or other network unless using a Virtual Private Network (VPN).
- Data from HMIS will not be downloaded to any remote access site at any time for any reason.
- All HMIS data (hardcopy) will be securely stored and/or disposed of in such a manner as to protect the information.
- Monitors need to be equipped with security screens when working in a public setting.
- System security provisions will apply to all systems where HMIS is accessed and the CHO employing the User will certify such systems for compliance.
- User must follow all confidentiality and privacy rules.
- User must assure access only for activities directly related to their job.
- User must allow for direct inspection of the remote access location by the Agency Administrator and compliance will be certified by the CHO.

Remote Access Authorization: Agreement to these remote access policies is included in the HMIS User Agreement, which must be signed in order to access HMIS.

Digital Data Retention Policy

Policy: Client PPI stored on any digital medium is purged, if no longer in use, 7 years after the data was created or last changed (unless a statutory, regulatory, contractual or other requirement mandates longer retention). Also, when digital medium where client PPI has been stored is to be decommissioned, it is reformatted more than once before reusing or disposing of the medium.

Explanation: PPI that is no longer needed must be removed in such a way as to reliably ensure the data cannot be retrieved by unauthorized persons. Because digital medium cannot be reliably erased via single reformatting, multiple (at least twice) reformatting is necessary to ensure the data cannot be retrieved.

Every three years digital files where PPI is stored are reviewed and client PPI that is no longer needed is deleted or otherwise removed in such a way as to reliably ensure the data cannot be restored.

At any time digital medium (computers, servers, data storage devices, etc.) where PPI has been stored is to be decommissioned, IT is instructed to reformat the medium at least twice prior to repurposing or disposing of said medium.

Data Breach Policy

Policy: HMIS Data is stored on BtiFocus operated servers. In the event of a data breach on those servers, CSB will work with BitFocus to determine the scale of the breach and take the necessary steps to notify those impacted.

Explanation: CSB does not have direct management over the servers used to store HMIS data. In the event of a breach, CSB will defer to BitFocus's data breach policy (below) and work with BitFocus to mitigate the damage and notify involved parties.

BitFocus Incident Response Policy

Scope

The scope of this policy includes all Information Systems that connect to the Bitfocus network, regardless of classification or location. These systems may include but are not limited to:

- Media including Electronic and Printed
- Desktop and Laptop Computers
- Servers
- Network Infrastructure
- Mobile Computing Devices
- "BYOD" - Bring Your Own Device

Applicability to Staff
This policy applies to those engaged in work for Bitfocus and includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Bitfocus are under the direct control of Bitfocus whether or not they are paid by Bitfocus. This policy applies regardless of on-site or remote work.

Applicability to External Parties
This policy applies to all Third-Party organizations serving as data owners of Bitfocus-owned information assets, as well as to all Third-Party organizations with access to information assets where Bitfocus serves as the owner or data owner of the assets.

Policy Statements

Acknowledgment of User Responsibilities
Appropriate training will be provided to all Bitfocus team members in order to maintain security awareness of the systems and data they are interacting with. This awareness helps personnel to identify potential security or privacy incidents. Workforce members are responsible for notifying PeopleOps or their direct manager of any suspected or confirmed security or privacy incidents. The designated members of the Incident Response team have additional responsibilities and duties documented in an Incident Response Procedure.
The Chief Operating Officer (COO), Chief Technology Officer (CTO), Legal, Information Security Officer (ISO), and the Information Privacy Officer (IPO) shall coordinate to determine when and who may contact the authorities, including law enforcement. The parties will analyze the legal requirements of the incident to determine the parties that will be contacted. All other outside contact by members of the Bitfocus workforce regarding incidents current or past is expressly prohibited.

Documentation of Incident Response Plan
The formal incident response procedure must be documented, tested, and appropriately communicated. The formal incident response procedures should address, but are not limited to, the following items:

- Specific roles and responsibilities for the members of the Incident Response team
- Key contact information for designated internal and external contacts (vendors, law enforcement)
- Workflows addressing the 5 phases of the response plan
- Detection and Identification
- Containment
- Eradication
- Recovery
- Lessons Learned
- External disclosure guidelines including those which are expressly and exclusively permitted to communicate with external parties, including customers, law enforcement, and media

Collection and Preservation of Evidence
Information Security Incidents may involve law enforcement or litigation which requires that evidence be appropriately collected and preserved. Bitfocus personnel should ensure that evidence is collected using appropriate tools and procedures so that a proper chain of custody is maintained when illegal activity is suspected. Assistance may be required of a third party to enable the proper collection and preservation of evidence. The procedures for

involving third parties for the collection and preservation of evidence must be established and included in Incident Response procedures.

Communication of Plan

To ensure all members of the Bitfocus workforce are able to effectively perform the Incident Response plan, role-appropriate training will be conducted on an annual basis.

Testing of Plan

The Incident Response plan shall be tested on an annual basis by conducting a simulated or "tabletop" exercise to ensure assigned resources are familiar with their responsibilities, contact information is current, and any lessons learned or new requirements have been implemented.

Exceptions

Appropriate Senior Management must provide written authorization for all exceptions to this policy. All exception requests, approved or denied, are documented and retained. Exceptions may be valid for up to 12 months and must be reviewed upon expiration. Expired exceptions must be re-authorized in order to remain in effect.

Policy Review

This policy will be reviewed on an annual basis by an appropriate member of Senior Management.

Incident Response Procedure

Objectives

When a security or technology disruption or data breach occurs, an investigation is started into the cause. Steps are taken to restore services as quickly as possible after containment of the activity. This procedure outlines how these investigations are carried out and documented.

Triaging an Incident

Incidents can be reported through various channels including internal and external users, system health monitoring alerts, security event alerts, and other monitoring controls. The Incident Response team determines if an incident has occurred based on the severity of a service disruption or data breach.

Documentation

If an incident has been identified, the incident is documented in a formal ticket or dedicated file. Restrictions are maintained on the visibility of incident documentation based on role and need. The minimum items captured throughout the treatment of the incident are as follows:

- Incident summary
- Detailed description
- Impact to business
- Priority (High, Medium, Low)
- Category (data breach, service disruption, etc.)
- Containment / Mitigation steps identified cause
- Outcome / Resolution

Investigation and Containment

The Incident Response team facilitates communication with responsible parties for investigating and containing the incident. The parties needed for the incident are identified and added to a communication channel dedicated to the incident (e.g. Slack channel, Zoom

call, etc.). Investigation into the incident proceeds and eradication activities are carried out until all parties feel the threat is appropriately contained.

Impact and Root Cause
Once containment of an incident is complete, an assessment is performed of the impact of the incident based on any breach of data or services disrupted. For data breaches, the assessment includes the number and types of records disclosed and to whom. For service disruptions, downtime and affected parties are captured. Further investigation is carried out to determine the root cause of the incident. This may involve the assistance of outside parties, including law enforcement. The Incident Management team facilitates mitigation activities to avoid the root cause from occurring in the future.

Communication
The impact of an incident may require communication to multiple external parties, including various levels of law enforcement, third-party partners, and internal and external users/customers. A list of these required communications is maintained by the Incident Response team.

Testing the Procedure
At least annually, the Incident Response team performs a tabletop exercise to test the Incident Response Procedure, verifying that all parties understand their roles and know what tools and resources are available to them.

4. Standard Operations

4.1 Access to HMIS

Agreements

Policy: The CEO (or other empowered officer) of any agency wishing to connect to HMIS signs an Agreement with CSB before any member of that agency is granted access.

Explanation: Only agencies that have agreed to the terms set out in the Agreement are allowed access to the HMIS. The Agreement includes terms and duration of access, an acknowledgement of receipt of the Policies and Procedures Manual, and an agreement to abide by all provisions contained therein. Each agency has an agency-level HMIS license.

CHOs are given a copy of the Agreement, the location of the Policies and Procedures Manual, and any other relevant paperwork in time for adequate review and signature. Once that paperwork has been reviewed and signed, agency users are trained to use HMIS. Once training and certification have been completed, each user is issued a username and password. Signing of the Agreement is a precursor to user access.

New User Licenses

Policy: If necessary, CHOs purchase additional User Licenses from BitFocus through CSB. The cost for User Licenses is determined by BitFocus, and is not be changed by CSB.

Explanation: As CHOs grow and the number of HMIS users increases, CHOs may need to purchase additional User licenses. This purchase can be made at any time. Licenses are purchased online, through the HMIS program, by the user with System Administrator privileges – the CSB Database Administrator. BitFocus then invoices CSB for the cost of the licenses.

CHOs wishing to purchase additional User Licenses must notify the CSB Database Administrator. The CSB Database Administrator purchases the User Licenses from BitFocus and notifies the CHO when the additional licenses are available.

Existing Licenses Redistribution

Policy: CSB conducts an annual reallocation process of unused licenses, to start in May of each year for the next Fiscal Year.

Explanation: The annual maintenance fee for each license is $105 ($420 for non-CSB funded projects), while the purchase cost for a new license is $280 ($595 for non-CSB funded projects). Given the high cost of purchasing and maintaining the licenses, it is not feasible for the agencies and CSB to keep a large amount of unused licenses in stock and it is more cost effective to reallocate licenses if they are needed, throughout the system.

CSB has an annual reallocation process of unused licenses, to start in May of each year for the next FY, per the following schedule:

Date	Step
Mid-May	Agencies receive email from CSB asking them for number of licenses that agency would need for next FY.
By June 1st	Agencies respond back to CSB with the projected number of licenses needed for the next FY.
Early June	Agencies receive email from CSB with summary of licenses needed for next FY and the available pool of unused licenses.
Mid-June	CSB re-allocates relinquished licenses to agencies who have requested new licenses for the new FY on a lottery basis, 1 license/agency, based on the available pool, until the pool is exhausted. Re-allocated licenses will be made available on July 1st.
Mid-June	If there are still licenses left in the pool, CSB will ask BitFocus to remove these licenses from the HMIS contract. If more licenses are needed, the respective agencies will be informed and the licenses ordered from BitFocus. Re-allocated and newly purchased licenses will be made available on July 1st.
July 1	CSB will invoice each agency for the annual maintenance cost, based on the number of current licenses for the upcoming FY, plus the full price for any newly purchased licenses.

At any point in the fiscal year, or if there are no available "reallocation" licenses, agencies can purchase new licenses for $280/license ($595 for non-CSB funded projects). In addition to the "new license fee" the agencies have to contribute the agreed upon annual maintenance fee/license, based on the current number of licenses, starting with the next fiscal year.

HMIS License Invoicing

Policy: CSB invoices each agency for each new license at the time of purchase and CSB invoices the applicable annual HMIS license support fees at the start of each fiscal year.

Explanation: BitFocus charges a one-time purchase fee for each license due at time of purchase and an annual support fee for each license purchased which they bill on a monthly basis to CSB .

The CSB Database Administrator calculates and submits to the CSB Finance Department the total amount to be invoiced to each agency for applicable license support fees at the beginning of each fiscal year. The applicable fees are re-examined in May of each year per CSB's license redistribution policy. When an agency purchases a new license, CSB Database Administrator submits to the CSB Finance Department the total of the one-time purchase price to be invoiced to the agency immediately. CSB Database Administrator issues the new license upon receipt of payment from the agency.

User Activation

Policy: Each new user is issued a username and password to access HMIS upon approval by the CHO, completion of training directed by the CHO, passing the HMIS certification test, and signing of the HMIS User Agreement.

Explanation: CHOs determine which of their employees have access to HMIS. Every user must receive appropriate HMIS training and certification before being issued a username and password.

The CSB Database Administrator and the Agency Administrators are responsible for training new users. The CSB Database Administrator provides training to Agency Administrators and users and will supplement this training as necessary. The initial username and password are only provided after completion of training and an HMIS certification test.

User Termination

Policy: HMIS Agency Administrators or supervisory staff should immediately notify the CSB Database Administrator regarding termination of an agency employee if they had HMIS access or if the employee no longer needs HMIS access.

Explanation: To safeguard the integrity of the HMIS staff, the CSB Database Administrator must be immediately informed when a user account should be deactivated. Failure to do so may result in a breach of contract.

HMIS User License Ownership

Policy: CSB maintains ownership of user licenses when a program terminates or discontinues use of HMIS or when CHOs decide to reduce their number of HMIS licenses. Licenses are redistributed yearly, through a CSB directed process.

Explanation: CSB retains ownership rights of all HMIS user licenses in the event that a program terminates or is otherwise discontinued from HMIS participation or when CHOs decide to reduce their number of HMIS licenses.

When a program discontinues HMIS participation or wishes to reduce their number of HMIS users/licenses the CSB Database Administrator deletes all user accounts affected and reallocates the licenses back to CSB for termination or redistribution. The CSB Database Administrator is responsible for managing the allocation of all user licenses within HMIS.

HMIS User Agreements

Policy: Each CHO User signs a HMIS User Agreement before being granted access to HMIS.

Explanation: Before being granted access to HMIS, each user must sign a HMIS User Agreement, stating that he or she has received training, will abide by the HMIS Policies and Procedures Manual and the CSB Privacy and Data Security Policy, will appropriately maintain the privacy, confidentiality, and security of client data, and will only collect, enter and retrieve data in HMIS relevant to the delivery of services to people in housing crisis in Columbus and Franklin County. Deviations from the User Agreement responsibilities must be reported to the CSB Database Administrator.

The HMIS system prompts new HMIS users with the HMIS User Agreement upon initial sign in. Electronic signature is required before full system access is granted. In the event a User Agreement is deleted or updated, a new agreement will need to be signed at next system login.

HMIS User Agreement Breach

Policy: CSB takes corrective action when a breach of the HMIS User Agreement is discovered.

Explanation: CSB enforces the Agreements signed by CHO Executive Directors/CEOs, Agency Administrators, and End Users.

When a breach is detected the user account of the person or persons involved is immediately deactivated by the CSB Database Administrator and notification sent to the Agency Administrator and/or the Agency Executive Director/CEO if necessary. All agency users may be deactivated for a serious breach. The CSB Database Administrator is responsible for notifying the CSB Associate Director of the agency breach.

Training

Policy: CSB provides adequate and timely HMIS training.

Explanation: CSB provides training in the HMIS software.

The CSB Database Administrator provides training to all new users via series of training videos that can be viewed on-demand. Agency Administrators are given additional training relevant to their position. Agency Administrators are expected to train new agency staff with the assistance of the HMIS training videos. The CSB Database Administrator provides periodic training updates and refreshers for all users, based on need. Once a new user completes training, they must complete a certification test to prove competency. This certification test incorporates many aspects of HMIS, requiring the user to create a client profile, create and update enrollments, enter specific data elements, create referrals, and add notes and system-wide alerts.

4.2 Data Collection

Required Data Collection/Fields

Policy: CHOs collect and enter into HMIS a required set of data variables for each client which is specified in the Agreement.

Explanation: Each Agreement will specify the data elements which must be collected for each client contact. CHOs may choose to collect and enter more client information for their own case management and planning purposes as is permissible under applicable law.

The Agreement contains a reference to a listing of data elements to be collected and entered in HMIS for each client contact in the HMIS Data Reference and Dictionary document.

Appropriate Data Collection

Policy: HMIS users only collect client data relevant to the delivery of services to people in housing crises in Columbus and Franklin County.

Explanation: The purpose of HMIS is to support the delivery of homeless and housing services in Columbus and Franklin County. The database should not be used to collect or track information not related to serving people in a housing crisis or served by the homeless system.

HMIS users must ask the CSB Database Administrator for any necessary clarification of appropriate data collection. CSB periodically audits pick-lists and agency specific fields to ensure the database is being used appropriately.

HMIS Protected Personal Data Collection and Privacy Protection

Policy: CSB and CHO ensure that all required client data will be captured in HMIS while maintaining the confidentiality and security of the data in conformity with all current regulations related to the client's rights for privacy and data confidentiality.

Explanation: Clients have the right to expect provider agencies to collect and manage their protected personal data in a manner that is secure and maintains their privacy. Clients have the right to know why agencies are electronically collecting their information and how it will be used.

Procedures:

1. The CHO has a privacy notice sign posted at each intake desk, minimally the one provided by CSB. The sign is posted in an area accessible and easily viewed by clients.
2. The CHO has a written privacy policy, minimally the one provided by CSB, to cover the electronic data collection, use and maintenance of the client's protected personal information. Clients are made aware of the privacy policy. The policy is posted on the agency's website and shared with the client upon request. The policy is reviewed at least annually and updated as needed. The CSB provided Privacy and Data Security Policy content must be included in the CHO's policy.
3. The CHO presents each client with a Client Acknowledgement for Electronic Data Collection form and informs the client about the provisions of the form. The CHO attempts to obtain a signed Client Acknowledgement for Electronic Data Collection form from each client before data is entered into the database and maintains this form on file in HMIS.
4. In case the acknowledgment form is not signed, the CHO still must electronically collect in HMIS any and all HMIS required data elements provided by the client to the agency. Based on current HUD regulations, CSB does not require client consent for the electronic data collection. The agency may also elect to implement a more restrictive client privacy policy than the one provided by CSB with respect to other data that is not HMIS required.
5. If the CHO has a more restrictive privacy policy than the one provided by CSB that disallows the collection and/or entry of the protected personal information (name, birth date and social security number) in HMIS without written client consent and the client refuses to provide written consent, the agency must enter the data by creating an Unnamed record for tracking purposes. This is a function within HMIS which involves entering the client's protected personal information which the system then uses to create a unique record identifier. The system then strips PPI out of the record.
   If the client consents with the electronic data collection, the agency must electronically collect in HMIS any and all HMIS required data elements provided by the client to the agency. Generally, the more restrictive HMIS related privacy policy should be implemented only by agencies that by law are required to have privacy standards more restrictive than the HUD standards (i.e. HIPAA).
6. The agency must provide CSB with its client privacy policy at the beginning of each CSB program year, with any updates made throughout the previous program year.

Educating Clients of Privacy Rights

Policy: The Agency Administrator maintains a current privacy policy and a privacy notice which includes the uses and disclosures of information.

Explanation: Clients have a right to expect service agencies to collect and manage their protected personal data in a manner that is secure and maintains their privacy.

The Agency Administrator ensures that a written privacy policy and a privacy notice is in place and up to date. The Agency Administrator also ensures that the privacy notice is posted in an area accessible and easily viewed by clients. The clients are informed of their rights under the privacy policy and receive the policy if requested. This policy is reviewed at least annually and updated as needed. CSB provides, as part of the Policies and Procedure Manual, the most current Privacy Policy and Privacy Notice. The CHOs should minimally adopt the documents provided by CSB.

Scanned Document Management

Policy: CSB is responsible for organization and management of the HMIS. It is necessary to standardize the way the document upload feature is utilized in order to ensure the information uploaded is organized and usable system-wide.

Explanation: CSB desires that essential client documentation be scanned and uploaded to HMIS. HMIS, as a client document repository is a useful tool for case managers in helping clients exit quickly from homelessness into stable housing. Client documentation is available quickly, avoiding delays in client services.

CSB seeks to provide a uniform HMIS which yields the most consistent data for client management, agency reporting, and service planning. To this end, CSB is providing the following guidelines for the utilization of the document upload feature.

- Files should be uploaded to the appropriate categories outlined below:
    - Data Forms – intake, annual, exit, etc.
    - Health and Medical – Disability certification, pregnancy verification, etc.
    - Homeless Documentation – Proof of homelessness, street verification, etc.
    - IHSP/Service Plan/HAST – Housing/goal plans
    - Income Documentation – Pay stubs, SSDI/SSI letters, self-certification of income, etc.
    - Lease – copy of client's lease, VAWA documentation, lead-based paint information, inspections
    - Personal Identification – State/federal ID, Birth certificate, Social Security Card, etc.
    - USHS – USHS application, USHS transfer packets, etc.
    - Miscellaneous – All other documentation that does not fit an above category (e.g. child custody documentation).

- Avoid duplication; if the document is already uploaded don't upload again.
- Naming Standards for uploading documents:
    - Format: Date. Program. Document Title.
    - Example: 03-02-23. HFL SRA. Income at Entry.
- Older documents should not be deleted when an updated version is uploaded, unless replacing a document that contains an error.

4.3 Data Entry

Timeliness of Data Entry

Policy: Clients must be enrolled into the appropriate HMIS program in a timely manner.

Explanation: To ensure consistency in how data is reported, all data must be entered by 9am the following day for shelters, and by the 4th working day of the following month for other program types.

All clients served by an emergency shelter must be entered into HMIS by 9am the following morning in order to accurately report on daily shelter capacity. All other project types must enter client data within 48 hours. All data corrections should be made by the 4th working day of the following month in order for accurate monthly reporting of program capacities and other key metrics.

Customizations

Policy: CHOs have the option of collecting additional data elements in HMIS.

Explanation: Custom, additional assessments may be created by the CSB Database Administrator at the request of CHO. Custom assessments contain questions that will be used to collect the additional data elements.

CSB Database Administrator, at the request and in collaboration with the Agency Administrators, will create custom assessments for CHOs.

Additional Customization

Policy: CHOs purchase any additional database customization directly from BitFocus. CSB does not provide additional customizations. However any proposed customizations must be approved by CSB.

Explanation: It is the responsibility of individual agencies to determine the best way to use HMIS for internal data collection, tracking, and reporting. This may include purchasing additional customization directly from BitFocus. CSB must review and approve any proposed customizations to ensure the integrity of the overall system.

CHOs provide a proposal to CSB and contact BitFocus directly with additional customization needs

Data Corrections

Policy: Data should not be changed once the System and Program Indicator Report (SPIR) has been published.

Explanation: Once data has been found compliant through the quarterly Quality Assurance review process the data is then utilized for funder, Continuum of Care, CSB Board and Community Reporting. To maintain the integrity of this reporting it is necessary to be able to provide numbers and statistics consistently over time.

CSB data entry standards require that all data is completely and accurately entered in HMIS by the 4th working day of the month after which there is a period of Quality Assurance reviews. It is the Agency Administrator's responsibility that data is entered completely and accurately on an ongoing basis through agency-level QA policies and procedures.

If data is found to be incomplete or incorrect during the QA period it is permissible to make changes up through the last day of the designated cure period. After compliance has been achieved no changes or corrections to the data which has been reviewed should be necessary.

Agency Administrators facilitate efficient and accurate data entry through training and monitoring of data entry personnel. Agency Administrators ensure data is accurately entered in a timely manner through rigorous quality assurance practices. If an agency discovers data inconsistencies after the quarterly QA period, the Agency Administrator should contact CSB's Database Administrator. In agreement with CSB's Database Administrator, changes may be allowed to data.

Annual Data Freeze

Policy: Annually, as of October 1st no changes are allowed to data records which have an exit date on or before the last day of the previous fiscal year. The fiscal year data is effectively "frozen" on an annual basis.

Explanation: Once data has been found compliant through the quarterly and annual Quality Assurance review process the data is then utilized for funder, Continuum of Care, CSB Board and Community Reporting. To maintain the integrity of this reporting it is necessary to provide consistent historical numbers and statistics over time.

CSB data entry standards require that all data is completely and accurately entered in HMIS by the 4th working day of the month after which there is a period of Quality Assurance reviews. At the end of a fiscal year, data for the entire year as well as the final quarter is reviewed for QA. It is the Agency Administrator's responsibility that

data is entered completely and accurately on an ongoing basis through agency-level QA policies and procedures.

If CSB and/or agencies discover a major inconsistency in previous fiscal year's data after October 1st the anomaly will be reviewed by CSB and action decided on a case by case basis.

Agency Administrators ensure through staff training and communication that changes will not be made to previous fiscal year data as of October 1st. Agency Administrators facilitate efficient and accurate data entry through training and monitoring of data entry personnel. Agency Administrators ensure data is accurately entered in a timely manner through rigorous quality assurance practices. If an agency discovers data inconsistencies in the previous fiscal year's data after the October 1st cutoff date, the Agency Administrator should contact CSB's Database Administrator. The anomaly will be reviewed by CSB and action decided on a case by case basis.

CSB issues data timeliness reports in conjunction with the quarterly QA to show data that was changed after the data correction period closes. These reports are sent quarterly to the Agency Administrators and Partner Agency CEOs.

Data Entry for Couples in Supportive Housing Programs

Policy: Data entry practices correspond with the target population of Supportive Housing programs/units.

Explanation: Couples present a challenge in data entry and reporting. The Columbus community encourages programs to serve couples, wherever possible, in the supportive housing programs.

For Permanent Supportive Housing units, an eligible client may share a unit with a non-eligible client. Because only the homeless, eligible clients must be accounted for, the couples are entered in HMIS as a household with the eligible client as the head of household. By the same token, if both members of the couple are eligible clients, then both need to be entered in HMIS and reported on as individuals.

Project Start Date vs Housing Move-In Date for PSH

Policy: Project Start Date should reflect the date the PSH provider begins working with the client and the enrollment/intake is completed. Housing Move-In Date should reflect the client's true housing move-in date.

Explanation: PSH providers should only enter the client into HMIS once the client is housed and back-date the Project Start Date.

For Permanent Supportive Housing the client should only be entered into HMIS once the client is housed. At that time, the Project Start Date should be back-dated to the client's enrollment (intake) date. The Housing Move-In Date should reflect the client's first date occupying the unit.

4.4 Quality Control

Data Integrity

Policy: HMIS users are responsible for the accuracy of their data entry.

Explanation: Individual users are responsible for the accuracy and quality of their own data entry.
In order to test the integrity of the data contained in HMIS, the CSB Database Administrator performs regular data integrity checks in HMIS. Any patterns of error are reported to the Agency Administrator. When patterns of error have been discovered, users are required to correct data entry techniques and will be monitored for compliance. CSB Database Administrator may require retraining in some cases.

Data Integrity Expectations

Policy: CHOs provide the following levels of data accuracy and timeliness:

- All data entered is accurate.
- Entry Dates and Exit Dates must match intake and exit forms within the client file and must be completed for each individual served.
- Blank, "Client Doesn't Know", "Client Refused", and "Data Not Collected" entries do not exceed, collectively, 5% per data field, per month.
- Data entry is completed in HMIS as real-time as possible. Data entry for shelter stays is completed by 9am each day for the previous night. Data entry for all other services provided is entered within 48 hours. Allowing for quality checks and corrections for any given calendar month-end, these must be completed within HMIS by the fourth working day of the following calendar month.

Explanation: Users enter client data as provided by the client and, preferably, confirmed by documentation. Of the fields required in the Agreement, less than 5% of fields will be left blank or marked as "Client Doesn't Know", "Client Refused", or "Data Not Collected" in one month. For example, if the last zip code field is left blank for 2% of clients, then the last zip code field should not have more than 3% of "Client Doesn't Know", "Client Refused", or "Data Not Collected" responses for clients entered during one month. When service records are added, no services are entered by programs that do not provide that type of service. For example, rental assistance should not be entered by a program that only provides emergency shelter. When service records for shelter stays are added, the client must meet the most basic

requirements of the program listed as providing shelter. For example, no clients listed as women should have shelter stays in shelters restricted to men. Agencies strive to complete entry data as real-time as possible. Data entry for shelter stays is completed by 9am each day for the previous night. Other services and items are entered within 48 hours of provision. Data entry for all services provided in one month must be accurately entered into HMIS by the fourth working day of the following month. For example, if April 30th falls on a Friday, data for April must be completed by close of business Thursday, May 6.

The CSB Database Administrator performs regular data integrity checks in HMIS. Any patterns of error at a CHO are reported to the Agency Administrator. When patterns of error have been discovered, users are required to correct data entry techniques and will be monitored for compliance. The CSB Database Administrator may require retraining in some cases.

Quality Assurance

Policy: CSB performs at least a quarterly quality assurance process for data entered by each CHO, related to HMIS.

Explanation: To keep the data integrity at the program and system level, CHOs and CSB perform a quality assurance process, at least quarterly, for data entered in HMIS.

All agencies are required to submit monthly the Client Duplicate report and inform the CSB Database Administrator of any client duplicates found, by the 4th working day following the end of a month (by secure email). This report becomes an integral part of the Monthly/Quarterly quality assurance process.

The Monthly QA review roster is based on the results of the initial run of the preceding Quarterly QA run. If an agency receives a noncompliant rating on the initial run of a quarterly QA review that agency will receive monthly reviews for the next two months.

- **The purpose of the Monthly QA is to encourage Agency Administrators to monitor their compliance status and catch problems early. We are also looking to focus an agency's attention on the QA problems.**
- Review for the previous month is run by the Agency Administrator by the 5th working day of the month.
- Results are emailed to the CSB Database Administrator by the 6th working day of the month.
- Administrators are expected to set their own schedule to review and effect a cure prior to the end of the third month of the quarter.
- Agencies will not have to do a monthly report for the third month of each quarter as this is when the Quarterly QA is run.

The Quarterly QA review schedule is 2-tiered:

- For the initial run, the Agency Administrator receive compliance results.
    - **The purpose of this step is to help Agency Administrators in determining the data integrity problems from the previous quarter and allow them sufficient time to correct the errors prior to inclusion in community reports.**
    - Review is run by the Agency Administrator based on the schedule distributed by the CSB Database Administrator.
    - QA Reports and details are sent (secure email) to the CSB Database Administrator by the scheduled due date.
    - Non-compliance will result in the Agency Administrator receiving a Non-Compliance email and a list of data corrections.
    - Non-compliant agencies are given **up to a week** to cure.
    - All noncompliant agencies on this run will be added to the Monthly QA Roster.
    - The 2nd run is only for those agencies found non-compliant in the 1st run; Agency HMIS Administrator and CEO receive the results.
    - **The purpose of the 2nd run is to make sure that all agencies are compliant with the minimal CSB data quality standards which in turn allow us to present the agency and system data in community reports and help the planning process to cover the ongoing homelessness related needs of our community.**
    - Agency Administrators will make corrections identified during the first run and then re-run and submit QA Repors and details to the CSB Database Administrator according to the QA Schedule.
    - Non-compliance results in a hard-breach letter being issued and signed by CSB's CEO.

Any agencies receiving a hard-breach letter may have funding suspended until a cure has been achieved. CSB will not include that agency's data in the Quarterly and/or Semi-Annual System and Program Indicator Report (SPIR) and the program will be issued a "program of concern". The System Results in the SPIR will be revised after the agency becomes compliant. Agency results will NOT be changed.

CSB will not include the agency data in the SPIR or any other reports if CSB staff is not confident in the reliability of that particular agency's data in HMIS, independent of the QA results.

The Coordinated Point of Access (CPOA) staff collects and enters the majority of the required data elements for each emergency shelter client, however all serving agencies remain accountable for the accurate representation of the client's data within HMIS. Programs receiving clients directed to their shelters via CPOA must review all required data elements and ensure all are entered and accurate as of the client's entry. When shelter staff discover an omission or mistake it should be promptly be corrected by the shelter HMIS staff.

Annual Review

Policy: CSB performs annual compliance monitoring reviews at each CHO of data processes related to HMIS.

Explanation: Reviews enable CSB to monitor compliance with the Policies and Procedures Manual and Agreements.

This review is part of the Annual Program Review and Certification process. The Monitoring Guide for Sub-recipients Program Review & Certification details the annual review.

4.5 Data Retrieval

Contributing HMIS Organizations (CHOs)

Policy: CHOs have access to retrieve any individual and aggregate data entered by their own programs. CHOs do not have access to retrieve aggregate data for other agencies or system-wide.

Explanation: Any data entered within an agency is available for reporting. Data entered by other agencies is not available, unless there are explicit data-sharing agreements in place.

When using the report writer or Looker report tool, users are only able to extract data from those records to which they have access. These modules will limit user access and only report data from records to which the individual user has access.

CSB Access

Policy: The Community Shelter Board has access to retrieve all data in HMIS. CSB does not access individual client data for purposes other than direct client service-related activities, reporting, maintenance, and checking for data integrity, with the exception of compliance with local or federal law enforcement warrants.

Explanation: CSB Data & Evaluation, Grants, Programs and Planning, and Housing departments have access to all data in the database. No other staff member of CSB has access to client-level data. CSB protects client confidentiality in all reporting.

CSB's Associate Director is responsible for ensuring that no individual client data is retrieved for purposes other than direct client service, reporting, maintenance, and performing data integrity checks. CSB's Associate Director will oversee all reporting for CSB.

Public Access

Policy: CSB addresses all requests for data from entities other than CHOs or clients. Individual client data is provided, upon request, to the CHO which entered the data, CSB's funder for the specific program for which individual client data is requested, outside organizations under contract with CSB or CHOs for research, data matching, and evaluation purposes, or the client him or herself. Proper authorization is required for all requests.

Explanation: Any requests for reports or information from an individual or group who has not been explicitly granted access to HMIS will be directed to CSB. No individual client data is provided to meet these requests without proper authorization.

All requests for data from anyone other than a CHO or a client are directed to the CSB Database Administrator. It is CSB's policy to provide aggregate data on homelessness and housing issues in Columbus and Franklin County. CSB also issues periodic public reports about homelessness and housing issues in Columbus and Franklin County. No individual client data is reported in any of these reports. CSB may share or allow client level data sharing with contracted entities as follows: CSB's or CHO's funder for the specific program for which individual client data is requested, outside organizations under contract with CSB or CHO for research, data matching, and evaluation purposes. The results of the analysis are always reported in aggregate form, client level data is not publicly shared under any circumstance.

Data Retrieval Support

Policy: Agencies create and run agency-level reports. CSB provides reports to agencies for their own use.

Explanation: The Agency Administrator has the ability to create and execute reports on agency-wide data. This allows agencies to customize reports and use them to support agency-level goals.

The Agency Administrator is trained in reporting by CSB and has access to on-demand videos outlining how to run reports, build custom reports, and interpret results of key reports. CSB's Database Administrator provides the template for reports specifically required by CSB. CSB's Data and Evaluation Team is a resource for report creation.

Appropriate Data Retrieval

Policy: HMIS users only retrieve client data relevant to the delivery of services to people in housing crises in Columbus and Franklin County.

Explanation: The purpose of HMIS is to support the delivery of homeless and housing services in Columbus and Franklin County. The database should not be used to retrieve or report information not related to serving people in a housing crisis.

Agency Administrators ask the CSB Database Administrator for any necessary clarification of appropriate data retrieval.

Inter-Agency Data Sharing

Policy: Data included in the Profile, Program Enrollments, and Services section of a client record is viewed by all users with the exceptions below. CHOs determine the security settings of the additional information entered in HMIS.

Explanation: When new clients and new service records are entered into HMIS, the information, by default is open to be viewed by users from other CHOs. Open sections of the record can be seen and changed by users from another CHO. There are a few agencies that are regulated by HIPAA Standards and those Agencies' records, by default, are closed. Closed sections of the record can neither be seen nor changed by users from another CHO. Regardless of status, all sections of each record will appear in aggregate reports

It is the intent of CSB to allow as much data sharing as appropriate and necessitated by the clients' needs and the services provided to meet those needs. Client profiles are set as "Open", as are service records and program enrollment records. HIPAA regulations, as followed by some of the CHOs take precedence over the above Policy and Procedure.

Currently, the following are the agencies that are entering and sharing information in HMIS:

Columbus Coalition for the Homeless	Home For Families	Southeast, Inc.
Community Development for All People	Huckleberry House	The Salvation Army
Community Housing Network	Lutheran Social Services/Faith Mission	U.S. Department of Veteran's Affairs
Community Shelter Board	Maryhaven	Volunteers of America
Equitas Health	Mount Carmel Health	YMCA of Central Ohio
Gladden Community House	National Church Residences	YWCA Columbus
Homefull	Netcare Access	

Agency Data Sharing

Policy: CHOs can share their data for research and data analyses purposes with prior approval by CSB.

Explanation: HMIS provides the ability to run reports and download client-level data by all CHOs. CHOs are encouraged to analyze their data and make programmatic decisions based on the information contained in HMIS. Data sharing must be done in conjunction with careful consideration of data confidentiality and privacy protocols.

The following steps are required by each CHO that wishes to share its data with an external contractor or vendor for research and data analysis purposes:

1. Data sharing will have to be approved by CSB
2. The provider will have to submit to CSB the data sharing agreement that will need to contain, at the minimum:
    a. Scope of the analysis/research that must be limited to the data that pertains to the individuals served by provider
    b. Information transmittal protocols
    c. Data confidentiality/privacy protocols
    d. Data handling after the analysis/research is complete

CSB Report Schedule

Policy: CSB provides a schedule or produced community reports.

Explanation: CSB maintains and updates a schedule of HMIS produced reports on their website at csb.org.

External Data Requests

Policy: CSB follows a standardized process for external data requests.

Explanation: External Data Requests are prioritized based on the scale and urgency of the request. A Data Request Form, outlining the scope of the data request is available on the CSB website at csb.org. An agency requesting data should complete the Data Request Form and submit to HMIS@csb.org. The typical data request process takes 6-8 weeks to complete.

4.6 Contract Termination

Initiated by CHO

Policy: The termination of the Agreement by the agency will affect other contractual relationships with CSB. In the event of termination of the Agreement, all data entered into HMIS remains an active part of HMIS, and records keep their original security settings.

Explanation: While agencies may terminate relationships with CSB and HMIS, the data entered remains part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in Columbus and Franklin County. The termination of the Agreement will affect any other contractual relationships with CSB.

Partner Agencies are required to participate in HMIS as a condition of their funding. For Partner Agencies, termination of the Agreement will be addressed in the context of the larger contract with CSB. For the Other CHOs terminating the Agreement, CSB will need to receive official notification with a date of termination of the Agreement. The CEO of CSB will notify the CSB Database Administrator. In all cases of termination of Agreements, the CSB Database Administrator will inactivate all users from that CHO on the date of termination of the Agreement.

Initiated by the Community Shelter Board

Policy: CSB will terminate the Agreement for non-compliance with the terms of that contract upon 30 days written notice to the CHO. CSB will require any HMIS violations to be rectified before the Agreement termination is final. CSB may also terminate the Agreement with or without cause upon 30 days written notice to the CHO and according to the terms specified in the Agreement. The termination of the Agreement by CSB may affect other contractual relationships with the CSB. In the event of termination of the Agreement, all data entered into HMIS will keep their initial security settings.

Explanation: While CSB may terminate the Agreement with the CHO, the data entered by the CHO prior to termination of contract remains part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in Columbus and Franklin County. The termination of the Agreement may affect other contractual relationships with CSB.

CSB Partner Agencies are required to participate in HMIS as a condition of their funding. For Partner Agencies, termination of the Agreement will be addressed in the context of the larger contract with CSB. When terminating the Agreement, the CEO of CSB will notify the CHO at least 30 days prior to the date of contract termination. The CEO of CSB will also notify the CSB Database Administrator. In all cases of termination, the CSB Database Administrator will inactivate all users from that CHO on the date of contract termination.

4.7 Programs in HMIS

Adding a New Program in HMIS

Policy: Agency Administrators follow the prescribed procedure to notify CSB 's Database Administrator prior to implementing a new program within HMIS. The CSB Database Administrator follows a standard formula when naming a new program within HMIS.

Explanation: When a new program is to be added or activated within HMIS the Agency Administrator is required to submit the requested information via the provided form prior to implementation. The CSB Database Administrator follows a standard pattern when creating a name for new programs being added to the HMIS and obtains approval from the Data & Evaluation department prior to implementation.

When a new program is to be added or activated within the HMIS, the following steps occur:

1. At least 60 days prior to the anticipated implementation date, Agency Administrators complete a "HMIS Program Implementation Request Form" and submit to the CSB Database Administrator.
2. If being newly added in HMIS, the CSB Database Administrator ensures that the following standard formula is used when creating a name within HMIS:
   Agency (Abbreviation) – CSB Contract/Program Name Program Type
   Example: CSB – Test Program PSH
3. The CSB Database Administrator present the completed request form and recommended program name to the Data & Evaluation Department for review and approval.
4. The CSB Database Administrator notifies the Agency Administrator of approval status at least 30 days prior to the requested HMIS implementation date.
5. The CSB Database Administrator assists the Agency Administrator with the HMIS implementation as needed.

Making Changes to Existing Programs

Policy: The Agency Administrator notifies the CSB Database Administrator of programmatic changes per the procedure below.

Explanation: Agencies must notify CSB of any program changes which affect data collection, data entry, data quality and/or data reporting. Agency Administrators accomplish this via the provided form which requests details such as (but not limited to) funding status, program type, quality assurance participation, program start and end date, capacity, etc.

1. The Agency Administrator notifies the CSB Database Administrator of any applicable programmatic changes to existing programs which may have an effect on data collection, data entry, data quality or data reporting (i.e. program expansion of capacity or scope; termination; deactivation; discontinuance of HMIS participation, etc.) Notification is made in writing at least 45 business days before the proposed implementation date of the change.
2. CSB's Database Administrator will circulate the completed form to the Data & Evaluation Department for review & comment.
3. Recommendations and timeline for assistance are returned to the agency no fewer than 10 business days prior to the requested implementation date.
4. The CSB Database Administrator assists with changes within HMIS as necessary.

While the Agency Administrators have the access to make changes to programs within the system, it is required that any changes first be reviewed with the CSB Database Administrator to determine the overall effect of the changes and to allow for documentation of changes as well as the arrangement of any necessary support.

Maintaining a HMIS Program Matrix

Policy: The CSB Database Administrator maintains a complete and up to date Program Matrix of HMIS.

Explanation: The Program Matrix is a complete index of all programs existing in HMIS, their status and other details such as (but not limited to) funding status, program type, quality assurance participation, program start and end date, etc.

The CSB Database Administrator records changes being made to any existing program in HMIS (termination, deactivation, etc.) and the addition of the new programs via the Program Matrix, upon receipt of the proper documentation from the Agency Administrator and after the finalization of the implementation plan. The CSB Database Administrator is responsible for ensuring the Program Matrix reflects any and all changes to programs within HMIS. The CSB Database Administrator reviews the Program Matrix with the Data & Evaluation Department on a quarterly basis.