HMIS Policies and Procedures

Columbus & Franklin County Continuum of Care

Fiscal Year 2027 | Effective Date: 4/17/2026

Administered by Community Shelter Board (CSB)

HMIS Lead, Collaborative Applicant, and Unified Funding Agency

Required under 24 CFR 578.7(b)(3) | HUD HMIS Data Standards

Table of Contents

1. Introduction

1.1 Governance Authority and Purpose

This HMIS Policies and Procedures Manual (P&P) is the operational governance document for the Homeless Management Information System (HMIS) of the Columbus & Franklin County Continuum of Care (CoC). It establishes the policies, procedures, roles, and responsibilities governing HMIS access, data collection, data quality, security, and system administration for all Covered Homeless Organizations (CHOs) participating in HMIS within the CoC.

Community Shelter Board (CSB) administers HMIS on behalf of the CoC in its capacity as the designated HMIS Lead, Collaborative Applicant, and one of fifteen Unified Funding Agencies (UFAs) in the United States under 24 CFR Part 578. As HMIS Lead, CSB is responsible for the day-to-day operation of HMIS, the development and enforcement of governance standards, and the provision of training, technical assistance, and monitoring to all CHOs. As Collaborative Applicant, CSB applies for and administers CoC Program funds on behalf of the CoC. As a UFA, CSB receives and subgrants multiple HUD funding streams, carrying compliance responsibility across the CoC's funded projects.

This Manual is required under 24 CFR 578.7(b)(3) and HUD's HMIS Data Standards and must be reviewed, revised, and approved by the CoC. It applies to all CHOs and their employees, volunteers, affiliates, contractors, and associates who access or enter data into HMIS, regardless of funding source.

1.2 HMIS Overview

HMIS is a locally implemented data system used to record and analyze client, service, and housing data for individuals and families experiencing or at risk of homelessness. HUD requires each CoC to maintain an HMIS that meets HUD's data collection, management, and reporting standards. The Columbus & Franklin County CoC's designated HMIS software is Clarity Human Services, developed and maintained by BitFocus.

Approximately 400 users across 30 agencies use HMIS to collect data for housing and homelessness-related programs throughout Franklin County. HMIS data supports individual client service coordination; program management and performance reporting by CHOs; community-level reporting to HUD, including the Point-in-Time Count, Housing Inventory Count, System Performance Measures, and Longitudinal Systems Analysis (LSA); and data-informed funding and resource allocation decisions by CSB and its partners.

CSB's HMIS operations are administered by the Data + Evaluation team, staffed by a full-time HMIS Database Manager, Data Analyst Manager, and Project + Data Analyst, reporting to the Deputy Chief, Housing + Data Systems.

The current HMIS is administered in full compliance with HUD's most recent HMIS Data Standards, effective October 1, 2025 (FY2026 version).

As one of fifteen Unified Funding Agencies nationally, CSB administers HMIS to a standard designed not only to meet HUD requirements but to serve as a model for strong, community-centered HMIS governance. CSB is actively building relationships with regional partners across central Ohio and participates in national HMIS working groups as it develops its capacity for broader regional leadership.

1.3 Governing Principles

HMIS exists to serve the people of the Columbus & Franklin County CoC. Its purpose is to support the coordinated, data-informed delivery of housing and homeless services across the region. HMIS is:

- a benefit to individual clients through enhanced service coordination, reduced duplication of intake, and more effective referrals across the CoC system
- a tool for CHOs in managing programs, documenting services, and meeting funder reporting requirements
- a resource for the CoC in planning, prioritizing, and evaluating the regional response to homelessness

CSB recognizes that the strength of HMIS depends on consistent, high-quality data entry by all participating organizations. Data quality is not a compliance exercise; it is the basis on which the CoC understands who it is serving, how well it is serving them, and where resources are most needed.

CSB also recognizes the primacy of client rights in the design and management of HMIS. Clients experiencing homelessness have a right to privacy, to understand how their data is used, and to receive services regardless of their willingness to share identifying information. The personal data of people experiencing homelessness must be collected, accessed, and used with respect, in strict compliance with applicable privacy law and HUD standards, and never for purposes unrelated to the delivery of housing and homeless services.

CSB follows, at all times, the CSB Privacy and Data Security Policy posted at csb.org and the HMIS Privacy Plan adopted by the Columbus & Franklin County CoC under 24 CFR 578.7(b)(3).

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. Frequently referred to as CSB's software vendor.

Clarity Human Services: A software application that is developed for human services client management. It is a web-based program that allows provider agencies to manage and secure client information. Clarity Human Services is the specific HMIS software utilized in the Columbus & Franklin County Continuum of Care (CoC).

Covered Homeless Organization (CHO): Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, or processes data on clients experiencing homelessness for an HMIS, as defined in HUD's 2004 HMIS Data and Technical Standards Final Notice. All CHOs are subject to the HMIS Final Notice requirements and the terms of the HMIS Agency Agreement.

Continuum of Care (CoC): The Columbus & Franklin County Continuum of Care is the HUD-designated planning body responsible for coordinating housing and homeless services in the region. The CoC designates an HMIS Lead, adopts governance documents, and oversees the community's response to homelessness. HUD funds CoC Program projects and HMIS implementations through the CoC.

Community Shelter Board (CSB): The Collaborative Applicant, HMIS Lead, and designated Unified Funding Agency (UFA) for the Columbus & Franklin County Continuum of Care. As Collaborative Applicant, CSB applies for and administers CoC Program funds on behalf of the CoC. As HMIS Lead, CSB administers HMIS and is responsible for governance, training, and compliance. As one of fifteen UFAs nationally, CSB receives and subgrants multiple HUD funding streams on behalf of the CoC.

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

Data Quality: The degree to which HMIS data is accurate, complete, timely, and consistent. Data quality is measured against locally defined benchmarks established in the HMIS Data Quality Plan and HUD's Data Quality Management Program (DQMP) framework.

Encryption: The translation of data from readable plain text into a coded format that can only be read by authorized parties with the correct decryption key. Encryption is required for all HMIS data transmitted over public networks and for locally stored extracted data.

End User (HMIS User): Any individual employed by or volunteering with a CHO who is authorized to access and enter data into HMIS on the agency's behalf. All HMIS Users must complete required training and sign the HMIS User Agreement before receiving system access.

Firewall: A security system, implemented in software, hardware, or both, that monitors and controls network traffic to protect against unauthorized access to a private network or system. CHOs must maintain active firewall software on all computers used to access HMIS.

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

Homeless Management Information System (HMIS): A locally implemented data system used to record and analyze client, service, and housing data for individuals and families experiencing or at risk of homelessness. HUD requires each CoC to designate an HMIS that complies with HUD's data collection, management, and reporting standards. The Columbus & Franklin County CoC's designated HMIS software is Clarity Human Services, administered by CSB as HMIS Lead.

Partner Agency: A CSB-funded organization that holds a Master Provider Agreement (MPA) with CSB and participates in HMIS as a CHO. Partner Agencies are subject to both the HMIS Agency Agreement and the HMIS-related terms of the MPA. Where those documents conflict on HMIS obligations, the HMIS Agency Agreement controls. Non-CSB-funded organizations that participate in HMIS are governed solely by the HMIS Agency Agreement.

Protected Personal Information (PPI): Any individually identifying information collected or maintained in HMIS that can be used to identify a specific individual, directly or indirectly. PPI includes name, date of birth, Social Security number, and other data that could identify a client. PPI is governed by HUD's HMIS privacy standards and the HMIS Privacy Plan adopted by the Columbus & Franklin County CoC. Note: HUD uses both "PPI" and "PII" (Personally Identifiable Information) in various guidance documents; this document uses PPI consistent with HUD's HMIS-specific standards.

HMIS Agency Administrator: The individual designated by each CHO as the primary HMIS point of contact and liaison between the CHO's end users and the CSB HMIS Database Manager. The HMIS Agency Administrator is responsible for user access management, agency-level data quality oversight, security compliance, training of new staff, and timely communication with the HMIS Database Manager on system issues, user changes, and program modifications. See Section 3.1 and the HMIS Agency Agreement for full responsibilities.

System Administrator: The CSB staff role with the highest level of administrative access in HMIS. The System Administrator has full access to all user accounts, system settings, and administrative functions. This role is held by the HMIS Database Manager, Data Analyst Manager, and Project + Data Analyst; it is not a CHO-level role.

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 Data Stewardship and System Authority

HMIS is administered by CSB on behalf of the Columbus & Franklin County CoC. Client-level data entered into HMIS is the collective asset of the CoC, held in trust by CSB as HMIS Lead. CSB, as the designated custodian of HMIS, has final authority over system

configuration, user access, data governance, and security. No CHO may alter system settings, extract data for unauthorized purposes, or use HMIS data outside the terms of its executed HMIS Agency Agreement.

CSB requires all CHOs to execute an HMIS Agency Agreement prior to receiving access to HMIS. The Agreement establishes data quality obligations, confidentiality requirements, user conduct standards, and the consequences of non-compliance. The Agreement is the binding instrument through which CSB exercises its HMIS Lead authority over all participating organizations, independent of any funding relationship.

Non-compliance with the terms of the HMIS Agency Agreement or with the policies and procedures in this Manual may result in suspension of individual user access, suspension of agency-level HMIS access, a required Data Quality Improvement Plan, or termination of the Agreement. For CSB-funded Partner Agencies, data quality failures may also be addressed in the context of the Master Provider Agreement.

2. Implementation Overview

2.1 Relationship to CHOs

Covered Homeless Organizations (CHOs) are all organizations authorized by CSB, in its capacity as HMIS Lead, to connect to HMIS for purposes of data entry, data editing, and data reporting. CHOs include CSB-funded Partner Agencies that hold a Master Provider Agreement with CSB, as well as non-CSB-funded organizations that participate in HMIS because it is required by their funder, because they have agreed to participate as part of the CoC's coordinated system, or because they serve people experiencing homelessness within the Columbus & Franklin County CoC geographic area.

Participation in HMIS by all CHOs is governed by the following documents. The HMIS Agency Agreement is the primary governing instrument for all CHOs. All documents listed below are incorporated by reference into the HMIS Agency Agreement and are binding on all CHOs:

- The HMIS Agency Agreement, Columbus & Franklin County CoC
- The HMIS Policies and Procedures, Columbus & Franklin County CoC
- The HMIS Local Data Dictionary, Columbus & Franklin County CoC
- The HMIS Privacy Plan, Columbus & Franklin County CoC
- Master Provider Agreement (MPA): for CSB-funded Partner Agencies only. Where MPA terms on HMIS obligations conflict with the HMIS Agency Agreement, the HMIS Agency Agreement controls.
- Master Provider Agreement (MPA): for CSB-funded Partner Agencies only, in addition to the HMIS Agency Agreement. Where MPA terms on HMIS obligations conflict with the HMIS Agency Agreement, the HMIS Agency Agreement controls. Non-CSB-funded organizations (including YHDP participants, Medical Respite

programs, and City-funded projects) participate under the HMIS Agency Agreement only, with no MPA.

These documents are subject to periodic updates. CSB will notify CHOs of material changes in accordance with the notice provisions of the HMIS Agency Agreement. All CHOs are required to comply with the current version of each document.

2.2 HMIS Participation as a Condition of CoC and ESG Funding

Consistent participation in HMIS by all CoC Program and Emergency Solutions Grant (ESG) recipients and subrecipients is required under 24 CFR 578.7(b)(4). CSB, in its capacity as Collaborative Applicant and Unified Funding Agency, enforces this requirement through the following mechanisms:

- All CoC Program subrecipients are required to execute an HMIS Agency Agreement with CSB as a condition of their award. Execution of the HMIS Agency Agreement and active participation in HMIS are conditions of each program year's Master Provider Agreement.
- All ESG recipients and subrecipients receiving funding administered by CSB on behalf of the City of Columbus or Franklin County are similarly required to participate in HMIS as a condition of their funding relationship, documented in their respective program agreements.
- New CoC and ESG-funded organizations are onboarded into HMIS prior to the start of their funded program period. The HMIS Database Manager coordinates onboarding with incoming recipients and subrecipients to ensure no gap in data collection at program launch.
- CSB monitors participation continuously through monthly data quality reporting. Organizations that fall out of active participation are contacted directly by the HMIS Database Manager. Persistent non-participation is escalated to the relevant program officer and, if unresolved, addressed through the corrective action and enforcement provisions of the applicable funding agreement.
- Non-CSB-funded organizations that are required to participate in HMIS by a federal program requirement (such as YHDP) must execute a standalone HMIS Agency Agreement with CSB before accessing the system. CSB maintains a current list of all participating organizations at https://www.csb.org/providers/hmis/.

2.3 Domestic Violence Service Providers: HMIS Exemption and Aggregate Data

Under federal law (42 U.S.C. 11385(e)) and HUD HMIS Data Standards, victim service providers whose primary mission is to serve survivors of domestic violence, dating violence, sexual assault, or stalking are prohibited from directly entering client-level data into HMIS. This prohibition exists to protect client safety and confidentiality.

Victim service providers operating within the Columbus and Franklin County CoC are therefore exempt from direct HMIS participation. This exemption applies only to organizations whose primary mission is to provide services to survivors of domestic violence, dating violence, sexual assault, or stalking, as defined in 24 CFR 578.3. Organizations whose primary mission encompasses broader community services are not VSPs under this definition and must apply the decision-tree analysis described in the following subsection. In lieu of client-level HMIS data entry, qualifying VSPs contribute aggregate, de-identified data to the CoC for inclusion in the annual Point-in-Time Count, Housing Inventory Count, and other required HUD reporting as follows:

- CSB maintains a formal process for collecting aggregate, unduplicated counts from victim service providers each reporting period. Through direct coordination with each VSP, CSB obtains counts of individuals and families served, by program type, for inclusion in applicable HUD reporting. No individually identifying information is collected through this process.
- Aggregate counts obtained from victim service providers are incorporated into CSB's CoC-wide HUD reports. This data is clearly attributed as aggregate data from non-HMIS-participating providers and is not co-mingled with client-level HMIS records.
- CSB maintains a current inventory of victim service providers operating within the CoC's geographic area, including those that are HMIS-exempt, in the HMIS Program Matrix described in Section 4.7.
- Victim service providers that wish to voluntarily participate in HMIS using a comparable database approved by HUD may do so in coordination with CSB. Any such arrangement must comply with applicable HUD guidance on comparable database use and must be documented in a written agreement with CSB.

2.4 Determining HMIS vs. Comparable Database Participation: Agencies Operating DV Programs

Not all agencies that serve survivors of domestic violence, dating violence, sexual assault, or stalking are exempt from HMIS participation. The exemption described above applies only to organizations that meet the federal definition of a Victim Service Provider: a private nonprofit organization whose primary mission is to provide services to survivors of domestic violence, dating violence, sexual assault, or stalking (24 CFR 578.3). Organizations whose primary mission encompasses broader community services — including organizations that operate one or more DV-specific programs alongside other programming — are not VSPs under this definition and are not exempt from HMIS.

CSB uses the HUD HMIS Comparable Database Decision Tree (HUD Exchange, January 2020) to make participation determinations for agencies whose HMIS status requires analysis. The decision tree applies the following sequential steps:

Step 1 — Primary mission test. If the agency is a VSP (primary mission is DV/SA/stalking services), all projects at that agency are prohibited from entering PII into HMIS, regardless of project type or funding source. The agency contributes aggregate data only, as described above.

Step 2 — FVPSA/OVC/OVW agency-wide funding test. If the agency is not a VSP but receives funding from the Family Violence Prevention and Services Act (FVPSA), Office for Victims of Crime (OVC), or Office on Violence Against Women (OVW) that is used agency-wide or for agency administrative purposes, all projects at that agency are prohibited from entering PII into HMIS.

Step 3 — FVPSA/OVC/OVW project-specific funding test. If the agency receives FVPSA, OVC, or OVW funding to support a specific project, that specific project cannot enter PII into HMIS. Other projects at the same agency that do not receive those funds must follow their own program's requirements.

Step 4 — Human trafficking funding test. Projects that receive Specialized Housing and Services for Victims of Human Trafficking funds cannot enter PII into HMIS.

Step 5 — Default rule. If none of the above conditions apply, the project must follow its funding program's requirements for HMIS participation. CoC Program and ESG-funded projects are required to enter data directly into HMIS.

For example: an agency whose primary mission is broad community services and which operates a DV-specific Rapid Re-Housing program funded through the CoC Program without FVPSA, OVC, or OVW funding is not a VSP and does not receive disqualifying funding. That program must participate in HMIS under its CoC Program funding requirements.

HMIS Agency Administrators at agencies operating DV-related programs should contact the HMIS Database Manager if there is any question about whether a specific project or funding source affects HMIS participation eligibility. CSB retains documentation of participation determinations for all programs in the HMIS Program Matrix.

2.5 Relationship to BitFocus

CSB maintains an annual contract with BitFocus for software maintenance, application support, and system hosting. Under this contract, CSB holds the master software license for HMIS and allocates individual user licenses to CHOs through the license management process described in Section 4.1. The HMIS Database Manager serves as the designated point of contact with BitFocus and is responsible for facilitating clear and timely communication between CHOs and BitFocus.

While most BitFocus communications will be routed through the HMIS Database Manager, CHOs requiring custom reports should first contact the CSB Data + Evaluation team, which creates custom reports by request as a standard service to participating agencies.

CHOs may independently contract with BitFocus for additional services outside the scope of what CSB administers, such as specialized system configuration or other vendor services not provided by CSB. In such cases, the individual agency assumes full responsibility for negotiating, funding, and managing all related communications with BitFocus. CSB is not a party to such arrangements and bears no responsibility for their outcomes.

2.6 Security Infrastructure

Clarity Human Services is maintained and hosted by BitFocus on cloud infrastructure. BitFocus employs a dedicated team of full-time security and operations professionals who ensure system availability, performance, and security. Infrastructure protections include physical data center safeguards, network firewalls, encrypted browser sessions, multi-factor authentication, and encryption of all data in transit and at rest. BitFocus maintains the security controls required by HUD's HMIS standards and CSB's contract with BitFocus.

CHOs are not required to interact directly with BitFocus for routine HMIS support. All system-level issues, outages, and security concerns should be reported to the HMIS Database Manager, who coordinates with BitFocus and notifies affected CHOs as appropriate. CHO-level security responsibilities are governed by Section 3.2 of this document.

3. Roles and Responsibilities

3.1 Project Organization

3.1.1 Project Management

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

Explanation: As the designated HMIS Lead, Community Shelter Board is responsible for all system-wide policies, procedures, communication, and coordination for the Columbus & Franklin County CoC. CSB works directly with BitFocus to implement system-wide changes, updates, and configurations as needed to maintain a compliant and functional HMIS.

CSB is committed to maintaining a uniform HMIS that produces consistent, reliable data to support client management, agency reporting, and service planning. Oversight of HMIS is structured as follows:

- HMIS Database Manager: Serves as the primary point of contact for all system-wide questions and issues.
- Back-up HMIS Database Manager: Designated by the Deputy Chief, Housing + Data Systems, to support continuity of HMIS operations.
- Deputy Chief, Housing + Data Systems: Provides direct supervisory oversight of the HMIS Database Manager.

- CSB President + CEO: As head of Community Shelter Board, holds ultimate responsibility for all final decisions regarding HMIS planning and implementation.

3.1.2 HMIS Agency Administrators

Policy: CSB-funded Partner Agencies holding a Master Provider Agreement must designate a minimum of two (2) HMIS Agency Administrators. Non-CSB-funded organizations must designate a minimum of one (1) HMIS Agency Administrator. All CHOs must also designate one named backup contact who can communicate with the HMIS Database Manager on urgent matters when the HMIS Agency Administrator is unavailable. CSB-funded Partner Agencies that are unable to meet the two-administrator requirement due to staffing constraints must notify the HMIS Database Manager in writing; CSB may approve an alternative designation of one HMIS Agency Administrator plus one named backup contact on a case-by-case basis.

Explanation: The HMIS 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 HMIS Database Manager 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 HMIS Agency Administrator trainings and regular meetings
- Participating as the advisors and consultants to the HMIS Database Manager

Designating a minimum of two HMIS contacts at each agency strengthens communication, ensures continuity of HMIS access during staff transitions, and distributes oversight responsibility for data quality and user compliance.

Each CHO must submit the names and contact information of its HMIS Agency Administrator(s) and backup contact to the HMIS Database Manager prior to or at execution of the HMIS Agency Agreement. Any changes to this information should be reported promptly. HMIS Agency Administrators receive additional training from the HMIS Database Manager to support their oversight responsibilities within the system.

3.1.3 User Access Levels

Policy: Access to HMIS is granted on the principle of least privilege. Each HMIS User receives only the level of access necessary to perform their assigned job responsibilities, and no greater.

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.

When adding new users, the HMIS Database Manager assigns access levels based on the principle of least privilege, granting only the permissions necessary for efficient job performance while prioritizing client data security. HMIS Agency Administrators should conduct a periodic review of their agency's active users and access levels to confirm that access remains appropriate and report any needed changes to the HMIS Database Manager.

3.1.4 CSB Communication with CHOs

Policy: The HMIS Database Manager is responsible for providing timely and relevant communication to all CHOs regarding HMIS.

The HMIS Database Manager proactively communicates system-wide changes and other relevant updates to agencies as needed, and strives to respond to all CHO inquiries within one business day of receipt. While complex issues may require additional time to resolve, a high level of availability and responsiveness is maintained.

General communications are directed to HMIS Agency Administrators, primarily via email. The HMIS Database Manager is also reachable by phone, and HMIS-related resources are available at https://www.csb.org/providers/hmis/ . HMIS Agency Administrators are responsible for ensuring that all relevant HMIS communications are shared with appropriate staff at their agency, including program managers, client intake workers, data entry staff, and others whose work is affected by system changes or policy updates.

3.1.5 CHO Communications with CSB

Policy: CHOs are responsible for directing all HMIS-related questions and support needs to the HMIS Database Manager. CHOs are encouraged to submit support requests via the dedicated email address, HMIS@CSB.org.

Explanation: Users at CHOs should first bring questions, needs, and issues to their HMIS Agency Administrator. If the HMIS Agency Administrator is unable to resolve the matter, they should contact the HMIS Database Manager by phone, email, or by submitting a support ticket to HMIS@CSB.org. The Data + Evaluation team reviews all incoming tickets and provides an initial response within one business day of first contact.

3.1.6 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 Clarity HMIS will be available 24 hours a day, 7 days a week, 52 weeks a year. However, no system achieves 100% uptime. In the event of planned maintenance or downtime, the HMIS Database Manager informs agencies as far in advance as possible to allow CHOs to plan accordingly.

In the event of unplanned or emergency downtime, BitFocus contacts the HMIS Database Manager. The HMIS Database Manager contacts HMIS Agency Administrators and informs them of the cause and duration of the interruption in service. The HMIS Database Manager logs all downtime for purposes of system evaluation.

3.1.7 Ethical Data Use

Policy: Data contained in HMIS is used solely to support the delivery of housing and homeless services within the Columbus & Franklin County CoC. Each HMIS User affirms the principles of ethical data use and client confidentiality by signing the HMIS User Agreement prior to receiving system access.

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 experiencing homelessness or housing instability within the Columbus & Franklin County CoC. 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 an HMIS User Agreement before being given access to HMIS. The user agreement may be completed electronically within Clarity. Any individual or CHO misusing or attempting to misuse HMIS data is subject to enforcement actions under the HMIS Agency Agreement, including suspension or revocation of system access.

3.1.8 CHO Grievances

Policy: CHOs contact the HMIS Database Manager 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, as HMIS Lead, has final decision-making authority over all aspects of HMIS administration.

CHOs bring HMIS problems to the attention of the HMIS Database Manager. If a matter cannot be resolved by the HMIS Database Manager, the HMIS Database Manager will take them to the Deputy Chief, Housing + Data Systems, and finally to the CSB President + CEO, whose decision is final on all HMIS matters.

3.1.9 Client Grievance

Policy: Clients who have a complaint about HMIS data entry, data access, or service coordination should bring it directly to the CHO with which they have a grievance. CHOs are responsible for responding to client concerns and must report all HMIS-related client complaints to the HMIS Database Manager.

Explanation: Each CHO is responsible for answering questions and complaints from its own clients regarding HMIS. Clients bring complaints directly to the agency with which they have a grievance. Agencies respond to client issues and send documentation of all HMIS-related client complaints to the HMIS Database Manager. The HMIS Database Manager logs all complaints, reports them to the Deputy Chief, Housing + Data Systems, and responds with appropriate action. Actions may include further investigation, clarification or revision of policies, or enforcement under the HMIS Agency Agreement. CSB will respond if users or agencies fail to follow the terms of the HMIS Agency Agreement, breach client confidentiality, or misuse client data.

Privacy Rights Grievances: A client who believes their privacy rights have been violated, including unauthorized collection, use, or disclosure of their Protected Personal Information (PPI), is subject to the grievance process established in Section 5.7.1 of this document. That process governs and supersedes the general complaint process above for privacy-specific grievances.

Under Section 5.7.1 of this document, privacy rights grievances must be:

- Submitted in writing to the CHO's designated privacy contact or directly to the CSB HMIS Database Manager at HMIS@CSB.org,
- Reviewed by CSB within 30 calendar days of receipt, and
- Responded to in writing with findings and, where applicable, corrective action.

CHOs must inform clients of the HMIS Privacy Plan grievance process upon request and must designate a privacy contact responsible for receiving and routing privacy-related grievances. Upon receipt of a privacy grievance, the CHO must promptly notify the HMIS Database Manager regardless of whether the client also contacts CSB directly.

3.1.10 CHO Hardware, Software, and Technical Support

Policy: CHOs are responsible for providing and maintaining their own hardware, software, and internet connectivity to access HMIS, as well as internal technical support for all equipment and connections used for that purpose. CSB does not provide hardware, IT troubleshooting, or network connectivity assistance.

Explanation: Clarity Human Services is a web-based application that runs in a standard web browser. No software installation is required beyond a current, supported browser and a reliable internet connection. CHOs may access HMIS from desktops, laptops, or other web-capable devices that meet the security requirements described in Section 3.2 of this document.

Each CHO is responsible for ensuring its staff have access to appropriate equipment and connectivity, and for providing or arranging internal technical support for hardware, software, and network issues. Questions about HMIS system access, user accounts, or data entry should be directed to the HMIS Agency Administrator and, if unresolved, to the HMIS Database Manager at HMIS@CSB.org. Hardware and network issues remain the responsibility of the CHO.

3.1.11 HMIS Documentation Updates

Policy: CSB maintains and distributes the HMIS governance document suite, user guides, and relevant forms for all HMIS Agency Administrators. All documents are kept current and in compliance with HUD policies and requirements.

Explanation: The HMIS Policies and Procedures provides HMIS Agency Administrators with guidance on maintaining compliance with HUD and CoC requirements. It documents roles and responsibilities, system access and security standards, data collection and quality requirements, and program management procedures applicable to all CHOs.

The HMIS Local Data Dictionary documents local system configuration, data element requirements, and workflow standards. HMIS training videos provide technical instruction for both HMIS Agency Administrators and end users. All documents and training resources are available at https://www.csb.org/providers/hmis/.

3.2 Security

3.2.1 User Access

Policy: The HMIS Database Manager 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 HMIS Database Manager 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 clients an accurate record of who has altered their 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 HMIS Database Manager 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.

3.2.2 User Changes

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

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

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

3.2.3 Passwords

Explanation: Clarity HMIS requires passwords to meet minimum complexity standards. All passwords must be at least eight characters and include at least one uppercase letter (A–Z), one lowercase letter (a–z), one number (0–9), and one non-alphanumeric character (!@#$()%^&*). Passwords may not contain: spaces; the word “clarity” or the name of the Clarity instance; the user’s first name, last name, or username; the sequences “ABC” or “123”; more than two consecutive identical characters; or any of the user’s three most recent prior passwords. Users are responsible for keeping their passwords confidential. On the 90th day after a password is set, Clarity requires the user to create a new password before accessing the system.

3.2.4 Password Recovery

Policy: HMIS users reset their own password via an automated email process. If the automated process is unavailable, users should contact their HMIS Agency Administrator, who will notify the HMIS Database Manager to reset the password manually.

Explanation: To reset a forgotten password, the user clicks the “Forgot Password” link on the Clarity HMIS login page. An automated email is sent to the address on file containing a reset link. The new password takes effect immediately and remains valid until the next scheduled 90-day expiration. If a user is locked out after multiple failed login attempts or the automated email process is not functioning, the user should notify their HMIS Agency Administrator promptly. The HMIS Agency Administrator will contact the HMIS Database Manager to resolve the issue. Password reset requests should not be sent directly to the HMIS Database Manager by end users; routing through the HMIS Agency Administrator ensures proper oversight and account security.

3.2.5 Inactive Users

Policy: HMIS user accounts that have not logged into Clarity HMIS for 120 days are automatically inactivated. Inactivation does not release a user's license; HMIS Agency Administrators must formally notify the HMIS Database Manager to reassign or terminate a license.

Explanation: Automatic inactivation protects the security of client data by preventing dormant credentials from remaining active. HMIS users receive an automated email notification two days before their account is scheduled to become inactive. HMIS Agency Administrators are responsible for monitoring inactivation notices on behalf of their agency's users and responding appropriately, particularly for staff on extended leave or in seasonal programs. A user whose account has been inactivated may request reactivation by submitting a request to HMIS@CSB.org. Users whose accounts have been inactive for one year or longer may be required to review HMIS training videos and complete practice assignment(s) in the Clarity HMIS Training site, a sandbox environment separate from the live system that allows users to practice data entry without affecting real client records. License reassignment or termination requires written notification from the HMIS Agency Administrator to the HMIS Database Manager; inactivation alone does not constitute notice of termination.

3.2.6 Extracted Data

Policy: HMIS users are responsible for maintaining the security of any client data extracted from HMIS and stored locally, including data used in custom reporting. Extracted PPI must not be transmitted over a public network unless encrypted. HMIS users must apply the same security standards to locally stored client data as to data within HMIS itself.

Explanation: Clarity HMIS allows authorized users to download client-level data to a local device via the report writer. Once extracted, that data is no longer protected by the system's built-in security controls; the user and the CHO are responsible for its protection. Extracted files containing PPI must be stored in a secure, access-restricted location and protected with encryption or strong password protection. Unencrypted PPI must not be transmitted via email, shared drives, or any other channel accessible outside a controlled, secure environment. When CSB initiates communication involving client data, it will use encrypted email; recipients must reply using the secure reply link in the encrypted message to maintain confidentiality. Questions about extracted data security should be directed to the HMIS Database Manager.

3.2.7 Data Access Location

Policy: All HMIS security requirements apply regardless of the physical location from which a user connects to HMIS or the device used to connect. Client confidentiality must be maintained in all access scenarios.

Explanation: Because Clarity HMIS is web-based, users may connect from a variety of locations and devices beyond their primary agency workstation. Location does not reduce any security obligation. Users connecting from outside the agency must follow the specific requirements of the Remote Access Policy in this section, including the requirement for a secure network and restrictions on downloading data to remote devices. The HMIS Agency Administrator is responsible for ensuring that all users at their agency understand that security standards are not relaxed when accessing HMIS from home, in the field, or from non-agency equipment.

3.2.8 Hardware & Software Security Measures

Policy: The HMIS Agency Administrator is responsible for ensuring that all hardware, software, and storage media used to access or store HMIS data are located in a secure area with access restricted to authorized staff and meet the minimum security standards listed in this section.

Explanation: Client data accessed through or extracted from HMIS must be protected at every point of contact, including the devices used to access the system and any media on which data is stored. The HMIS Agency Administrator ensures that all devices and storage media used by their agency for HMIS access or data storage meet the following minimum requirements:

Computers and devices used to access HMIS:

- Password-protected screen lock that activates automatically after a period of inactivity
- Operating system and software kept current with security updates
- Antivirus and anti-malware software with automatic updates enabled
- Individual network firewall enabled

Storage media containing extracted PPI:

- Encrypted using current encryption standards
- Access restricted to authorized personnel only

These requirements apply to all devices used for HMIS access, including personally owned devices used under the Remote Access Policy. The HMIS Agency Administrator is responsible for certifying that devices meet these standards and for reporting any security concerns to the HMIS Database Manager.

3.2.9 Multiple Log-on Restriction Policy

Policy: Individual HMIS users may not be logged into HMIS from more than one device or location at a time. Simultaneous access to client-level data from multiple locations is prohibited.

Explanation: Clarity HMIS enforces single-session access. If a user attempts to log in from a second device, the system automatically ends the prior session. This protects client data accountability by ensuring each session is tied to a single authenticated user at a single location. HMIS users must not attempt to circumvent this control, and HMIS Agency Administrators must report any suspected attempts to the HMIS Database Manager.

3.2.10 Remote Access Policy

Policy: HMIS is intended to be accessed from the CHO's primary network and devices. Remote access, meaning access from outside the CHO's primary network or from a personally owned device, is permitted only when all requirements of this section are met.

The HMIS Agency Administrator is responsible for ensuring that all remote access by their agency's users complies with this policy.

Explanation: Because Clarity HMIS is web-based, users can access client-level data from virtually any internet-connected device. This flexibility requires clear boundaries to protect client data. Users who access HMIS remotely assume the same obligations as when accessing from the agency; location and device do not reduce any security requirement. The HMIS User Agreement, which every user must sign before receiving access, incorporates these remote access requirements by reference.

Requirements for remote access to HMIS:

- HMIS may only be accessed on secure, private networks. Access on unprotected, public, or free networks is prohibited unless the user is connected through a Virtual Private Network (VPN) provided or approved by the CHO's IT infrastructure. Personal consumer VPN services do not satisfy this requirement.
- Extracted PPI must not be downloaded to a remote device unless the device meets the security requirements of the Hardware and Software Security Measures section and the Extracted Data section of this document.
- Screen privacy filters must be used when accessing HMIS in any public or shared setting where the screen may be visible to unauthorized individuals.
- Users may access HMIS remotely only for activities directly related to their job responsibilities.
- All hardware and software used for remote HMIS access must meet the security standards in the Hardware and Software Security Measures section of this document. The CHO is responsible for certifying compliance.

Remote Access Authorization: Agreement to these remote access requirements is incorporated into the HMIS User Agreement, which must be signed before a user receives access to HMIS.

3.2.11 Digital Data Retention Policy

Policy: Client PPI stored on any digital medium must be retained for a minimum of seven (7) years from the date the data was created or last modified, or for as long as required by applicable federal, state, or contractual requirements, whichever is longer. PPI that has met its retention period and is no longer required for reporting or compliance purposes must be purged in a manner that reliably prevents unauthorized retrieval. When any digital medium containing PPI is decommissioned, it must be sanitized using at least two full reformats or, for solid-state drives and flash storage, a verified secure erase or physical destruction method, prior to repurposing or disposal.

Explanation: The seven-year retention period is a minimum standard intended to align with federal reporting obligations and common grant compliance requirements. Retention is measured at the individual record level, not on a fixed organization-wide review cycle. A record created in 2020 becomes eligible for purging in 2027; a record last modified in 2023

is not eligible until 2030. CHOs should conduct periodic reviews of locally stored data to identify records that have met the retention threshold and remove them as part of routine data hygiene.
Single reformatting does not reliably erase data from traditional magnetic hard drives because residual traces can persist and may be recoverable. At least two full reformats are required for such media. Solid-state drives (SSDs), USB drives, and other flash storage devices cannot be reliably sanitized through reformatting alone; secure erase functions built into the device firmware, or physical destruction, must be used instead. The HMIS Agency Administrator or CHO designee is responsible for ensuring that all decommissioned devices and media, including cloud-synced and network storage that has held PPI, are properly sanitized and that the method used is documented.

3.2.12 Data Breach Policy

Policy: Any HMIS user who discovers or suspects a security incident or data breach must report it to their HMIS Agency Administrator immediately. The HMIS Agency Administrator must notify the HMIS Database Manager at HMIS@CSB.org within 24 hours of becoming aware of the incident. End users may also contact the HMIS Database Manager directly at HMIS@CSB.org, but direct contact does not substitute for notification through the HMIS Agency Administrator. CHOs must not independently investigate, remediate, or communicate externally about a suspected breach pending direction from CSB.

Explanation: HMIS data is stored on BitFocus-operated servers. CSB does not have direct management over those servers. In the event of a breach, CSB will coordinate with BitFocus under BitFocus's Incident Response Policy to determine the scale of the incident, contain it, and notify affected parties. CHOs play a critical role in early detection; users are often the first to notice unusual system behavior or unauthorized data access. Prompt reporting gives CSB and BitFocus the best opportunity to contain an incident before it expands. Until CSB provides direction, CHOs must preserve any relevant records, avoid altering affected systems, and refrain from contacting external parties, including clients or media, about a suspected breach. The full incident response framework, including detection, containment, eradication, recovery, and communication procedures, is documented in the HMIS Security Plan — Columbus & Franklin County CoC, adopted by the CoC under 24 CFR 578.7(b)(3) and available at https://www.csb.org/providers/hmis/.

4. Standard Operations

4.1 Access to HMIS

4.1.1 Agreements

Policy: An authorized representative of any organization wishing to connect to HMIS must execute an HMIS Agency Agreement with CSB before any user at that organization is granted system access. Execution of the HMIS Agency Agreement is a prerequisite for all HMIS access.

Explanation: The HMIS Agency Agreement establishes the terms of access, data quality obligations, confidentiality requirements, and the consequences of non-compliance. It incorporates by reference the full FY2027 HMIS governance document suite, including this Policies and Procedures document, the HMIS Privacy Plan, the HMIS Data Quality Plan, and the HMIS Local Data Dictionary. Each CHO is charged an annual agency-level HMIS participation fee, billed at the start of each fiscal year, which covers the CHO's organizational access to the system. Individual user licenses are separate and are described in the sections that follow. CSB provides CHOs with access to the HMIS Agency Agreement and the full governance suite for review in advance of execution. User account setup and training follow execution of the Agreement; see Section 3.2 (User Access) for the user onboarding process. HMIS participation fees apply to all CHOs; see the HMIS License Invoicing section below for the fee framework. Current fee amounts are published in the annual HMIS Participation Fee Schedule, available at https://www.csb.org/providers/hmis.

4.1.2 New User Licenses

Policy: CHOs that require additional user licenses beyond those currently allocated must submit a request to the HMIS Database Manager. CSB purchases additional user licenses from BitFocus on the CHO's behalf and bills the cost to the CHO at rates established by CSB's contract with BitFocus.

Explanation: Each HMIS user requires an individual user license to access the system. As CHO staffing changes, additional licenses may be needed. CHOs do not purchase licenses directly from BitFocus; all license transactions are managed by the HMIS Database Manager. To request additional licenses, the HMIS Agency Administrator should contact the HMIS Database Manager, who will confirm availability, process the purchase with BitFocus, and notify the CHO when the additional licenses are ready to assign. License costs are billed to the CHO upon acquisition. Additional licenses may be requested at any time during the fiscal year.

4.1.3 Existing Licenses Redistribution

Policy: Each year CSB conducts a structured reallocation process to redistribute unused licenses before new ones are purchased. The process begins in May and is complete by July 1 of the new fiscal year. All CHOs are expected to participate by responding to CSB's annual license count inquiry within the timeframe specified.

Explanation: License purchase and annual maintenance costs are determined by CSB's contract with BitFocus and vary by funding tier; see the HMIS License Invoicing section for the current fee schedule. Given the cost of purchasing and maintaining licenses, it is not feasible for CHOs or CSB to carry a large inventory of unused licenses. The annual reallocation process described below provides a structured mechanism to redistribute unused licenses before new ones are purchased.

The reallocation process follows the schedule below.

Date	Step
Mid-May	Agencies receive an email from CSB requesting the number of licenses the agency will need for the upcoming fiscal year. Agencies must respond by June 1st.
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 matches the available pool of relinquished licenses against agency requests. If the pool meets or exceeds total demand, all requesting agencies receive their requested licenses from the pool. If demand exceeds the available pool, CSB distributes pool licenses by lottery, allocating one license per requesting agency per round until the pool is exhausted; agencies whose full request was not met may purchase the remaining licenses at the current rate. Any pool licenses not claimed by requesting agencies are removed from the HMIS contract by CSB. If additional licenses are needed beyond the pool, CSB orders them from BitFocus and notifies the affected agencies. All reallocated and newly purchased licenses are made available on July 1st.
July 1	CSB invoices each agency for the applicable annual maintenance fees based on the number of active licenses for the upcoming fiscal year, plus the one-time purchase fee for any newly acquired licenses. See the HMIS License Invoicing section for fee types and rates.

At any point in the fiscal year, or if there are no available reallocation licenses, agencies may purchase new licenses at the current per-license rate. In addition to the one-time purchase fee, the agency will be charged the applicable annual maintenance fee for each new license starting with the next fiscal year. Current rates are published in the annual HMIS Participation Fee Schedule, available at https://www.csb.org/providers/hmis/ .

4.1.4 HMIS License Invoicing

Policy: CSB invoices each CHO for HMIS participation fees on an annual basis at the start of each fiscal year and for individual user license purchases at the time of acquisition. Fees are structured on a two-tier basis based on whether the CHO receives funding through CSB's Unified Funding Agency (UFA) designation.

Explanation: HMIS participation fees reflect the cost of system access, maintenance, and support. Community Shelter Board receives federal housing and homeless funding, a portion of which is applied to subsidize HMIS participation fees for CSB-funded Partner Agencies operating under the UFA. CHOs that do not receive funding through CSB's UFA are subject to the standard, unsubsidized fee schedule. Both tiers are charged the same agency-level participation fee; the difference between tiers applies to user license rates and the project administration fee, which is charged only to non-CSB-funded CHOs.

The following fee types apply to all CHOs unless otherwise noted, with rates varying by funding tier:

- Agency License Fee: An annual fee charged to each participating CHO, billed at the start of each fiscal year, covering organizational access to HMIS regardless of the number of users.

- User License Fee: An annual maintenance fee per individual user license, billed at the start of each fiscal year based on the number of active licenses held by the CHO. CSB-funded Partner Agencies are charged a subsidized rate; non-CSB-funded CHOs are charged the standard rate.

- New User License Purchase Fee: A one-time fee charged when a new user license is purchased mid-year, in addition to the applicable annual maintenance fee beginning the following fiscal year.

- Reporting License Fee: An annual fee required for all HMIS Agency Administrators and for any user who needs reporting access. Reporting licenses provide the access necessary to run system and agency-level reports within HMIS.

- Project Administration Fee: An annual fee applicable only to non-CSB-funded CHOs operating specific federally funded project types, including SSVF, GPD, PATH, and HHS-funded licenses. Non-CSB-funded CHOs that served fewer than 50 clients in the prior fiscal year may submit a written appeal to the HMIS Database Manager to request a waiver of this fee. Waivers are granted at CSB's discretion.

Current fee amounts for each tier are published annually in the HMIS Participation Fee Schedule at https://www.csb.org/providers/hmis/. Fee amounts are subject to change based on CSB's contract with BitFocus and are reviewed annually. The HMIS Database Manager issues HMIS invoices and sends a copy to the CSB Finance Department and to the agency. New user licenses are activated upon invoice issuance; payment is due per CSB's standard invoicing terms.

All HMIS participation fees are assessed on an annual basis. Fees are not pro-rated for partial-year participation and are not refunded if a CHO reduces its license count, terminates its Agreement, or discontinues HMIS participation during the fiscal year for which fees have been billed.

4.1.5 User Activation

Policy: Each new HMIS user is issued a username and password upon CHO approval, completion of required training, passing the HMIS certification assessment, and signing the HMIS User Agreement. No user may access HMIS until all four prerequisites are met.

Explanation: CHOs determine which staff members require HMIS access and are responsible for initiating the onboarding process through their HMIS Agency Administrator. CSB uses a train-the-trainer model: the HMIS Database Manager trains HMIS Agency Administrators, who are then responsible for training end users at their agency. The HMIS Database Manager provides supplemental training and technical assistance as needed. Training resources, including instructional videos and the Clarity HMIS Training site sandbox environment, are available at https://www.csb.org/providers/hmis/ . Once the HMIS Agency Administrator confirms that a user has completed training and the certification assessment, the HMIS Database Manager issues the user's credentials and configures access at the appropriate level per the principle of least privilege.

4.1.6 User Termination

Policy: The HMIS Agency Administrator must notify the HMIS Database Manager immediately when an agency employee with HMIS access leaves the organization, is reassigned to a role that no longer requires HMIS access, or is otherwise terminated from HMIS use. Prompt notification is a mandatory obligation under the HMIS Agency Agreement.

Explanation: A former employee or unauthorized user retaining active HMIS credentials represents a direct risk to client data security and a potential data breach. Delayed notification is a violation of the HMIS Agency Agreement and may result in suspension of agency-level access. Upon receiving notice, the HMIS Database Manager deactivates the user account, preserves associated data records in accordance with data retention requirements, and returns the license to CSB's pool for reallocation. Note that deactivation of a user account does not release the license fee already billed for the current fiscal year; see the HMIS License Invoicing section.

4.1.7 HMIS User License Ownership

Policy: CSB retains ownership of all HMIS user licenses. When a CHO reduces its license count, terminates its HMIS Agency Agreement, or discontinues participation in HMIS, all associated licenses revert to CSB for termination or reallocation through the annual redistribution process.

Explanation: Because CSB holds the master software agreement with BitFocus and is responsible for all license management, user licenses are CSB's asset regardless of which CHO they are assigned to. When a CHO reduces its license count or exits HMIS, the HMIS Database Manager deactivates all affected user accounts and returns the licenses to CSB's pool. Returned licenses are available for reallocation to other CHOs through the annual redistribution process described in the Existing Licenses Redistribution section. Reducing or relinquishing licenses does not entitle a CHO to a refund of fees already billed for the current fiscal year; see the HMIS License Invoicing section.

4.1.8 HMIS User Agreements

Policy: Each HMIS user must sign an HMIS User Agreement before being granted access to HMIS.

Explanation: The HMIS User Agreement requires each user to affirm that they have completed required training; will abide by the HMIS Policies and Procedures — Columbus & Franklin County CoC and the CSB Privacy and Data Security Policy; will maintain the privacy, confidentiality, and security of client data; and will only collect, enter, and retrieve data in HMIS for purposes directly related to the delivery of services to people experiencing homelessness or housing instability within the Columbus & Franklin County CoC.
The HMIS system presents the User Agreement to each new user upon initial login. Electronic signature is required before full system access is granted. If the User Agreement is updated, users must sign the revised agreement at their next system login before access is restored.

4.1.9 HMIS User Agreement Breach

Policy: When a breach of the HMIS User Agreement is discovered, CSB will take corrective action, which may include immediate deactivation of the user account, suspension of agency-level HMIS access, a required Data Quality Improvement Plan, or termination of the HMIS Agency Agreement, depending on the severity of the breach.

Explanation: Upon discovery of a User Agreement breach, the HMIS Database Manager immediately deactivates the account of the user or users involved and notifies the HMIS Agency Administrator. Where the breach involves unauthorized disclosure of client PPI, misuse of HMIS data, a pattern of policy violations, or any conduct that places client data at risk, the HMIS Database Manager also notifies the CSB President + CEO and the Deputy Chief, Housing + Data Systems. In cases of serious or systemic breach, all agency-level HMIS access may be suspended pending investigation and remediation. The full range of enforcement actions available to CSB is documented in the HMIS Agency Agreement. All breaches are logged by the HMIS Database Manager and reported to the Deputy Chief, Housing + Data Systems regardless of severity.

4.1.10 Training

Policy: All HMIS users must complete required training and pass a certification assessment before receiving HMIS access. CSB uses a train-the-trainer model: the HMIS Database Manager trains HMIS Agency Administrators, who are responsible for training end users at their agency. Users whose accounts have been inactive for one year or longer may be required to complete retraining before access is restored.

Explanation: CSB provides on-demand training resources to support the train-the-trainer model. The HMIS Database Manager trains each HMIS Agency Administrator on system navigation, data entry standards, agency-level administration, and data quality requirements. HMIS Agency Administrators are then responsible for training new end users at their agency using CSB-provided training videos and other resources available at https://www.csb.org/providers/hmis/. The HMIS Database Manager is available to provide supplemental training and technical assistance as needed.

Before receiving HMIS credentials, each new user must complete all required training and pass a certification assessment demonstrating competency in HMIS. The assessment requires the user to create a client profile, create and update enrollments, enter required data elements, create referrals, and add notes and system-wide alerts. The assessment is completed in the Clarity HMIS Training site, a sandbox environment separate from the live system, so practice entries do not affect real client records.

The HMIS Database Manager provides training updates and refreshers when HUD issues changes to HMIS data standards, when CSB implements system updates that affect data entry workflows, or when data quality monitoring identifies a need for targeted retraining. Updates are communicated to HMIS Agency Administrators at quarterly HMIS Agency Administrators meetings and via direct email for time-sensitive changes. Users whose accounts have been inactive for one year or longer may be required to complete retraining before access is restored; see the Inactive Users section.

4.2 Data Collection

4.2.1 Required Data Collection/Fields

Policy: CHOs must collect and enter into HMIS all data elements required for each client, program enrollment, and service interaction, as specified in the HMIS Local Data Dictionary, Columbus & Franklin County CoC and applicable HUD data standards.

Explanation: Required data elements vary by project type and funding source and are documented in the HMIS Local Data Dictionary, Columbus & Franklin County CoC, which is available at https://www.csb.org/providers/hmis/ . The HMIS Agency Agreement incorporates the Local Data Dictionary by reference; CHOs are bound to collect and enter all elements specified for their project types as a condition of HMIS participation. CHOs may collect and enter additional client information for their own case management and planning purposes, provided such collection is consistent with applicable privacy law and the data collection limitations in the HMIS Privacy Plan.

4.2.2 Appropriate Data Collection

Policy: HMIS users may only collect and enter client data that is relevant to the delivery of services to people experiencing homelessness or housing instability within the Columbus & Franklin County CoC. HMIS must not be used to collect or track information unrelated to that purpose.

Explanation: Appropriate data collection means collecting information that is reasonably necessary to deliver, coordinate, or report on services to clients within the CoC's homelessness response system. Examples of appropriate data include: client demographics required by HUD, service dates and types, housing outcomes, income and benefits, and disability status as required for program eligibility. Examples of data that would not be appropriate include: information collected solely for internal agency marketing or fundraising purposes, data about clients' legal history beyond what is required for program eligibility, or any data element not authorized by the HMIS Local Data

Dictionary or HUD standards for the CHO's project type. When in doubt, HMIS Agency Administrators should direct questions about appropriate data collection to the HMIS Database Manager before creating or enabling custom fields. CSB reviews picklists and agency-specific fields as part of the quarterly and annual data quality review cycles to ensure the system is being used appropriately.

Document: See Section 7 of this document (HMIS Data Quality Plan) for data quality standards and the full list of approved data collection elements by project type.

4.2.3 HMIS Protected Personal Data Collection and Privacy Protection

Policy: CHOs must collect all required client data in HMIS while protecting the confidentiality and security of that data in compliance with applicable law, HUD's HMIS privacy standards, and the HMIS Privacy Plan, Columbus & Franklin County CoC. CHOs that are subject to more restrictive privacy requirements by law, such as HIPAA-covered entities, must comply with those requirements in addition to HUD standards.

Explanation: Clients have the right to know that their data is being collected electronically, to understand how it will be used, and to receive services regardless of whether they consent to share identifying information. The following requirements apply to all CHOs participating in HMIS:

Privacy notice: Each CHO must post a privacy notice at each client intake location in an area that is accessible and clearly visible to clients. The notice must meet the minimum requirements of HUD's HMIS privacy standards and the HMIS Privacy Plan. CSB provides a model privacy notice that satisfies these requirements; CHOs may use the CSB notice or an equivalent that meets the same standards.

Written privacy policy: Each CHO must maintain a written client privacy policy that covers the electronic collection, use, and maintenance of PPI in HMIS. The policy must address at minimum the elements required by HUD's HMIS privacy standards. CHOs may use or adapt the CSB Privacy and Data Security Policy as their organizational policy. The policy must be made available to clients upon request and reviewed at least annually. CHOs must submit their privacy policy to CSB at the start of each program year, including any updates from the prior year.

Client consent: CHOs must present each client with a Client Acknowledgement for Electronic Data Collection form and explain its provisions before entering data into HMIS. CHOs must seek a signed acknowledgement from each client and retain the signed form on file. Under current HUD regulations, client consent is not required for HMIS data collection; if a client declines to sign, the CHO must still collect and enter all required HMIS data elements provided by the client.

Unnamed records: If a CHO operates under a privacy policy more restrictive than HUD standards, such as one required by HIPAA or another applicable law, and that policy

prohibits entering a client's identifying information without written consent, and the client declines to consent, the CHO must enter the client using the Unnamed record function in Clarity HMIS. This function creates an anonymized record that protects the client's identifying information from routine access while still capturing required non-identifying data elements for reporting purposes.

4.2.4 Educating Clients of Privacy Rights

Policy: CHOs must actively inform clients of their privacy rights at the point of service. Intake staff and case managers are responsible for explaining the agency's privacy practices and the client's rights regarding their data in HMIS. The HMIS Agency Administrator is responsible for ensuring that the mechanisms for client education are in place, current, and consistently used.

Explanation: Clients must be informed of their privacy rights before or at the time their information is collected. This includes explaining why data is being collected electronically, how it will be used and shared within the CoC system, and what rights the client has regarding their data. Each CHO must maintain a current written privacy policy and posted privacy notice that together satisfy the requirements of the HMIS Privacy Plan, Columbus & Franklin County CoC. The HMIS Agency Administrator ensures these materials are up to date, posted in a visible location accessible to clients, and available upon request. The privacy policy must be reviewed at least annually and updated as needed. CSB provides model privacy documents that meet the minimum HUD standards; CHOs may use these materials or equivalent documents that satisfy the same requirements.

4.2.5 Scanned Document Management

Policy: CHOs must follow CSB's standardized procedures for uploading client documents to HMIS to ensure uploaded materials are consistently organized and accessible system-wide.

Explanation: Uploading essential client documentation to HMIS supports efficient case management by making key documents available quickly, reducing delays in service delivery and housing placement. Files must be uploaded to the appropriate category using the naming standard described below. Do not upload duplicate documents; if a document is already on file in HMIS, do not upload it again. Older documents must not be deleted when an updated version is uploaded, unless the original contains an error.

Upload categories:

- Data Forms: intake, annual, exit, and similar program forms
- Health and Medical: disability certification, pregnancy verification, etc.
- Homelessness Documentation: proof of homelessness, street outreach verification, etc.
- Individualized Housing Stability Plan (IHSP)/Service Plan/Housing Assistance and Support Tool (HAST): housing and goal plans

- Income Documentation: pay stubs, SSDI/SSI award letters, self-certification of income, etc.
- Lease: copy of client's lease, VAWA documentation, lead-based paint information, inspection reports
- Personal Identification: state or 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)

Naming standard for uploaded documents:

Format: MM-DD-YYYY. Program Abbreviation. Document Title.
Example: 03-02-2023. HFL SRA. Income at Entry.

4.3 Data Entry

4.3.1 Timeliness of Data Entry

Policy: CHO staff must enter client data into HMIS according to the following standards: emergency shelter client records must be entered by 9:00 a.m. the morning following the night of service; all other project types must enter client data within 48 hours of the service interaction; and data corrections must be completed by the 4th business day of the month following the month in which the data was originally entered.

Explanation: Timely data entry is essential to accurate reporting at both the agency and CoC levels. Each standard reflects the reporting requirements of the project type it governs:

- Emergency shelter: Client records must be entered by 9:00 a.m. the morning following the night of service. This standard applies every day of the year, including weekends and holidays, because emergency shelter occupancy is reported on a daily basis and late entry directly affects the accuracy of shelter capacity and utilization data.
- All other project types: Client data must be entered within 48 hours of the service interaction. This applies to project start dates, exit dates, annual assessments, and all required data elements. The 48-hour standard supports timely coordination of services across the CoC and ensures data is available for reporting within the required windows.
- Data corrections: Corrections to previously entered data must be completed by the 4th business day of the month following the month in which the data was originally entered. This allows for accurate monthly reporting of program capacities and other key metrics. Corrections identified after this window must still be made but may affect prior reporting periods.

Failure to meet timeliness standards may result in data being excluded from monthly or quarterly reports, a non-compliance finding in the quality assurance process, or a formal

non-compliance notice. See the Quality Assurance section for the full consequences of timeliness non-compliance.

4.3.2 Customizations

Policy: CHOs may request custom assessments within HMIS to collect additional data elements relevant to their program operations. Custom assessments are built by the HMIS Database Manager in collaboration with the requesting CHO and must not conflict with HUD data standards or the integrity of system-wide reporting. This section covers custom assessments built within the existing HMIS system; for CHO-purchased modifications from BitFocus, see the Additional Customization section.

Explanation: Custom assessments allow CHOs to collect program-specific data beyond the standard HUD-required elements, such as locally defined intake questions, service tracking fields, or case management notes specific to a program's target population. To request a custom assessment, the HMIS Agency Administrator should contact the HMIS Database Manager with a description of the data to be collected and its intended use. The HMIS Database Manager will review the request, confirm it is consistent with the Appropriate Data Collection requirements in this document, and build the assessment in collaboration with the HMIS Agency Administrator. Custom assessments are subject to review as part of CSB's annual system audit.

4.3.3 Additional Customization

Policy: CHOs that require database modifications beyond what CSB can provide through custom assessments may purchase additional customization directly from BitFocus. CSB does not fund or build such customizations. CSB approval is required before a CHO engages BitFocus for any additional customization, to ensure the proposed changes do not compromise the integrity of the system or conflict with CoC-wide data standards.

Explanation: Additional customization covers modifications to the HMIS system itself, such as custom-built modules, workflow changes, or interface modifications, that go beyond the custom assessment fields the HMIS Database Manager can configure within the existing system. These modifications are purchased directly from BitFocus by the CHO and are distinct from the in-system custom assessments described in the Customizations section above. To initiate an additional customization, the HMIS Agency Administrator must first submit a written proposal to the HMIS Database Manager describing the proposed modification and its intended purpose. CSB will review the proposal and respond with approval or concerns before the CHO contacts BitFocus. Engaging BitFocus prior to receiving CSB approval is not permitted.

4.3.4 Data Corrections

Policy: Data corrections are permitted during the quarterly QA cure period. Once the cure period has closed and data has been found compliant, corrections to that data must not be made without prior approval from the HMIS Database Manager. Corrections to prior fiscal year data after October 1st require prior written approval from the HMIS Database Manager and are subject to CSB review on a case-by-case basis; the HMIS Database

Manager will not approve post-freeze corrections that would alter finalized HUD report submissions without consulting the Deputy Chief, Housing + Data Systems.

Explanation: Maintaining consistent historical data is essential for accurate funder, Columbus & Franklin County CoC, CSB Board, and community reporting. Once data has passed the quarterly QA review and the cure period has closed, that data is considered finalized for the reporting period. CHOs must make all corrections during the designated cure period, which is established by the QA schedule distributed by the HMIS Database Manager.

If data is found to be incomplete or incorrect during the QA period, CHOs must make all necessary corrections before the last day of the cure period. Corrections submitted after the cure period has closed will not be reflected in reports already generated from that period.

If a CHO identifies a data error after the cure period has closed, the HMIS Agency Administrator must contact the HMIS Database Manager before making any changes. The HMIS Database Manager will review the error and determine whether a post-period correction is appropriate. Corrections to prior fiscal year data after October 1st require written approval from the HMIS Database Manager and are subject to CSB review on a case-by-case basis.

4.4 Quality Control

4.4.1 Data Integrity

Policy: HMIS users are responsible for the accuracy and completeness of their own data entry. HMIS Agency Administrators are responsible for monitoring data quality at the agency level and ensuring that staff data entry practices meet the standards established in this document.

Explanation: Data integrity depends on accurate, complete, and timely entry at the individual user level and consistent oversight at the agency level. Errors in individual records compound into system-level inaccuracies that affect CoC-wide reporting, performance measurement, and funding decisions. Both users and HMIS Agency Administrators have a direct role in maintaining the quality of the CoC's shared data asset.

The HMIS Database Manager conducts regular data integrity checks, separate from and in addition to the quarterly QA review process. These checks identify patterns of error across agencies and project types. When a pattern of error is identified, the HMIS Database Manager reports the findings to the affected HMIS Agency Administrator and works with the agency to determine the cause and required corrective action. Corrective action may include targeted retraining, data corrections within the applicable cure period, or, for persistent or serious errors, the remediation steps described in the Training and HMIS User Agreement Breach sections.

4.4.2 Data Integrity Expectations

Policy: CHOs must meet the following minimum data accuracy and completeness standards. Timeliness standards are established in the Timeliness of Data Entry section. Users must enter client data as accurately as possible, confirmed by supporting documentation where available.

Entry dates and exit dates must match the corresponding intake and exit forms in the client file and must be completed for every individual served.
Blank, "Client Doesn't Know," "Client Refused," and "Data Not Collected" responses must not collectively exceed 5% of entries per required data field.

Service records must accurately reflect the services the program actually provides. Programs must not enter service types they do not offer, and clients must meet the program's basic eligibility criteria for any service or shelter stay recorded.

Explanation: The 5% threshold applies collectively across all four non-answer response types for each required field. For example, if 2% of entries for the last permanent zip code field are left blank, no more than 3% of entries for that field may be marked as "Client Doesn't Know," "Client Refused," or "Data Not Collected." The combined total across all four non-answer types must not exceed 5% for any single required field.

Service record accuracy is a separate but equally important data quality standard. Entering service types a program does not provide, or recording shelter stays for clients who do not meet a program's eligibility criteria, corrupts system-wide reporting on service capacity and utilization. HMIS Agency Administrators are responsible for ensuring that service records entered by their agency's users accurately reflect actual program operations and client eligibility.

4.4.3 Quality Assurance

Policy: CSB performs a quality assurance process at least quarterly for data entered by each CHO, evaluating completeness, accuracy, and timeliness against the benchmarks established in the HMIS Data Quality Plan, Columbus & Franklin County CoC. CSB may exclude agency data from community reports at any time if CSB does not have confidence in the reliability of that agency's data, independent of QA results.

Explanation: The QA process operates at two levels: a quarterly review conducted for all CHOs, and a monthly review for CHOs that did not achieve compliance in the most recent quarterly run. Both levels use a two-run structure designed to give HMIS Agency Administrators an opportunity to review and correct errors before results are finalized.

Client Duplicate Report: All CHOs must submit the Client Duplicate report to the HMIS Database Manager by the 4th business day of each month via secure email to HMIS@CSB.org. CHOs must identify and report any duplicate client records found. The Client Duplicate report is a required component of both the monthly and quarterly QA processes.

Quarterly QA Run 1: CSB distributes the QA schedule to all HMIS Agency Administrators. Each HMIS Agency Administrator runs the quarterly QA review according to that schedule and receives compliance results for their agency. The purpose of the first run is to identify data integrity issues from the prior quarter and give agencies sufficient time to make corrections before data is included in community reports. QA reports and supporting details must be submitted to the HMIS Database Manager by the scheduled due date via secure email. CHOs that do not achieve compliance on the first run receive a non-compliance notice from the HMIS Database Manager identifying required corrections and are given one week to cure. All CHOs that remain non-compliant after the first run are added to the Monthly QA Roster for the following two months.

Quarterly QA Run 2: The second run applies only to CHOs that were non-compliant on the first run. The HMIS Agency Administrator and the agency's President + CEO receive the results. The purpose of the second run is to confirm that all CHOs meet the minimum CSB data quality standards required for agency and system data to be included in community reports and used in the Columbus & Franklin County CoC's planning process. HMIS Agency Administrators must make all corrections identified in the first run and resubmit QA reports to the HMIS Database Manager according to the QA schedule. CHOs that remain non-compliant after the second run receive a formal hard-breach letter issued and signed by CSB's President + CEO. CHOs receiving a hard-breach letter may have funding suspended until compliance is achieved. CSB will not include that CHO's data in the quarterly System and Program Indicator Report (SPIR), the Semi-Annual SPIR, or any other community report, and the program will be designated a program of concern. SPIR system-level results will be revised once the CHO achieves compliance; agency-level results will not be revised retroactively.

CPOA and Emergency Shelter Data: Coordinated Point of Access (CPOA) staff collect and enter the majority of required data elements for emergency shelter clients. However, all shelter programs remain accountable for the accuracy and completeness of client data in HMIS. Programs receiving clients directed through CPOA must review all required data elements and ensure they are entered and accurate as of the client's program entry date. When shelter staff identify an omission or error, it must be corrected promptly by the shelter's HMIS staff.

Monthly QA: CHOs placed on the Monthly QA Roster following a non-compliant quarterly first run receive monthly reviews for the two months following that quarterly run. The Monthly QA is designed to encourage HMIS Agency Administrators to monitor their compliance status and identify problems early, before the next quarterly review.

Each HMIS Agency Administrator on the Monthly QA Roster must run the review for the prior month by the 5th business day of the current month and submit results to the HMIS Database Manager by the 6th business day. HMIS Agency Administrators are expected to resolve any non-compliance identified before the end of the third month of the quarter, at

which point the Quarterly QA run replaces the monthly review. CHOs on the Monthly QA Roster are not required to submit a monthly report for the third month of each quarter.

4.4.4 Annual Review

Policy: CSB performs an annual compliance monitoring review at each CHO covering data entry practices, data quality, security procedures, and adherence to the HMIS Agency Agreement and this Policies and Procedures document.

Explanation: The annual review gives CSB a structured opportunity to assess each CHO's HMIS practices beyond what the quarterly QA process measures. Reviews may identify training needs, data quality patterns, security gaps, or agreement compliance issues that require corrective action. Findings are documented and shared with the HMIS Agency Administrator. Unresolved findings may result in a corrective action plan or, for serious non-compliance, the enforcement actions described in the HMIS Agency Agreement. The annual review is conducted as part of CSB's Annual Program Review and Certification process, documented in the Monitoring Guide for Sub-recipients Program Review and Certification.

4.4.5 Covered Homeless Organizations (CHOs)

Policy: CHOs may retrieve individual and aggregate data for their own programs. CHOs do not have access to individual client records entered by other agencies and may not retrieve other agencies' program-level data without an explicit data-sharing agreement.

Explanation: All data entered by a CHO is available for that CHO's own reporting purposes. The system limits each user's access to records within their assigned programs; the report writer and Looker report tool return data only from records to which the individual user has access. Aggregate system-wide data is available through CSB's public reports at https://www.csb.org/providers/hmis/.

4.5 Data Retrieval

4.5.1 CSB Access

Policy: 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, system maintenance, and data integrity checks, except as required by local or federal law enforcement warrant.

Explanation: CSB's Data + Evaluation, Grants, System Effectiveness, and Housing teams have access to all data in HMIS as required to fulfill their respective program, reporting, and system oversight responsibilities. No other CSB staff have access to client-level data. CSB protects client confidentiality in all reporting and does not publish individual client data in any form.

CSB's Deputy Chief, Housing + Data Systems is responsible for ensuring that no individual client data is retrieved for purposes outside those named in this policy and for overseeing all HMIS reporting conducted by CSB.

4.5.2 Public Access

Policy: CSB manages all requests for HMIS data from entities other than CHOs or clients. Individual client data may be disclosed only to: the CHO that entered the data; CSB's or the CHO's funder for the specific program to which the data pertains; organizations under contract with CSB or a CHO for research, data matching, or evaluation purposes; or the client themselves. Proper authorization is required for all disclosures. Individual client data is never publicly reported under any circumstance.

Explanation: All requests for data from any individual or organization that has not been explicitly granted access to HMIS must be directed to the HMIS Database Manager. CSB provides aggregate data on homelessness and housing issues in the Columbus & Franklin County CoC through periodic public reports; no individual client data appears in these reports. When client-level data is shared with contracted research or evaluation partners, results must be reported in aggregate form only. The External Data Requests section describes the process for submitting a formal data request.

4.5.3 Data Retrieval Support

Policy: HMIS Agency Administrators create and run agency-level reports. CSB provides required report templates and, through the Data + Evaluation team, serves as a resource for report creation and interpretation.

Explanation: The HMIS Agency Administrator has the ability to create and run reports on all data entered by their agency, supporting customized agency-level analysis and program planning. CSB provides training on the report writer and access to on-demand instructional videos covering how to run standard reports, build custom reports, and interpret key report outputs. The HMIS Database Manager provides templates for reports specifically required by CSB. The Data + Evaluation team is available as a resource for agencies that need assistance with report creation or data interpretation.

4.5.4 Appropriate Data Retrieval

Policy: HMIS users may only retrieve client data for purposes directly related to the delivery of services to people experiencing homelessness or housing instability within the Columbus & Franklin County CoC. HMIS must not be used to retrieve data for purposes unrelated to that mission.

Explanation: Appropriate data retrieval means running reports and accessing records for program planning, client service coordination, and required reporting purposes. Retrieving client data for unrelated purposes, sharing extracted data outside the CHO without CSB approval, or using HMIS data for commercial or non-service purposes is prohibited. HMIS Agency Administrators should direct questions about appropriate data retrieval to the HMIS Database Manager.

4.5.5 Inter-Agency Data Sharing

Policy: By default, a client's Profile is visible to and editable by users from all participating CHOs. Program Enrollments and program-specific data entry are visible to other CHOs but editable only by the agency that entered them. Certain agencies are subject to more restrictive access settings as described below.

Explanation: Client Profile data is open by default and can be viewed and edited by users from other CHOs, supporting coordinated service delivery and reducing duplicate intake across the CoC. HMIS Agency Administrators should ensure their users understand that another CHO's user may update information in a client's Profile. Program Enrollments and program-specific data entry, however, are editable only by the agency that created them; other CHOs may view this information but may not alter it. Regardless of open or closed status, all record data is included in aggregate system-wide reports.

CSB supports data sharing to the fullest extent appropriate to client needs and service coordination within the Columbus & Franklin County CoC. See the HMIS Privacy Plan, Columbus & Franklin County CoC for additional guidance on data sharing and client privacy rights.

The current list of CHOs participating in HMIS and sharing data system-wide is maintained at https://www.csb.org/providers/hmis/ and updated as agencies join or leave the system.

4.5.6 Agency Data Sharing

Policy: CHOs may share data about the clients they serve for research or data analysis purposes, with prior written approval from CSB. CSB approval must be obtained before any data is transferred to an external party.

Explanation: When a CHO wishes to share client-level data with an external contractor, vendor, or research partner, the following process applies:

1. CSB approval: The CHO must submit a written request to the HMIS Database Manager describing the purpose of the data sharing arrangement. CSB must approve the request before any data is transferred. The review process typically takes six to eight weeks to complete.
2. Data sharing agreement: The CHO must submit to CSB a fully executed data sharing agreement prior to any data transfer. The agreement must include at minimum:
    a. Scope of the analysis or research, limited to data pertaining to the individuals served by the provider.
    b. Information transmittal protocols.
    c. Data confidentiality and privacy protocols.
    d. Data handling and destruction procedures after the analysis or research is complete.

Results of any approved data sharing arrangement must be reported in aggregate form only. Individual client data must not be included in any published or publicly shared output

under any circumstance. See the Public Access section for CSB's broader policy on individual client data disclosure.

4.5.7 External Data Requests

Policy: CSB follows a standardized process for all external data requests, including requests for aggregate HMIS data from researchers, policymakers, media, and other non-CHO parties.

Explanation: External data requests are reviewed and prioritized based on the scope, purpose, and urgency of the request. Requests with direct relevance to CoC planning, funder reporting, or community benefit are prioritized. CSB publishes a schedule of community-facing HMIS reports and makes aggregate data available to the public through those reports; no individual client data is included in any public report. Organizations seeking data beyond what is available in published reports must complete the Data Request Form, available at https://www.csb.org/providers/hmis/ and submit it to HMIS@CSB.org. The typical data request process takes six to eight weeks to complete. CHOs seeking reports on their own program data should use the reporting tools available within HMIS or contact the HMIS Database Manager; the external data request process is intended for parties without direct HMIS access.

4.6 Contract Termination

In all cases of Agreement termination, whether initiated by the CHO or by CSB, data entered into HMIS prior to termination remains part of the system with its original security settings unchanged. Data is not deleted upon termination. This ensures the database maintains longitudinal accuracy and supports community planning for homelessness response services within the Columbus & Franklin County CoC.

4.6.1 Initiated by CHO

Policy: A CHO wishing to terminate its HMIS Agency Agreement must provide written notice to CSB by email to HMIS@CSB.org, including the intended date of termination. Termination of the HMIS Agency Agreement may affect other contractual relationships with CSB.

Explanation: Partner Agencies are required to participate in HMIS as a condition of their funding under the Master Provider Agreement; for Partner Agencies, termination of the HMIS Agency Agreement will be addressed in the context of the broader MPA. For non-CSB-funded CHOs, termination is effective on the date specified in the written notice. The HMIS Database Manager will inactivate all user accounts associated with the CHO on the stated termination date.

4.6.2 Initiated by Community Shelter Board

Policy: CSB may terminate the HMIS Agency Agreement for non-compliance with its terms upon 30 days' written notice to the CHO. CSB will require any HMIS violations to be rectified before termination becomes final. CSB may also terminate the Agreement without

cause upon 30 days' written notice. Termination of the Agreement by CSB may affect other contractual relationships with CSB.

Explanation: Termination by CSB may arise from persistent non-compliance with data quality standards, security requirements, or the terms of the HMIS Agency Agreement, and will be pursued only after other corrective measures have been attempted. For Partner Agencies, termination of the HMIS Agency Agreement will be addressed in the context of the Master Provider Agreement and the broader funding relationship. CSB will deliver the 30-day written termination notice to the HMIS Agency Administrator on file. The HMIS Database Manager will inactivate all user accounts associated with the CHO on the date of termination.

4.7 Programs in HMIS

4.7.1 Adding a New Program in HMIS

Policy: HMIS Agency Administrators must notify the HMIS Database Manager at least 60 days before implementing a new program in HMIS, using the electronic HMIS Program Implementation Request Form available at https://www.csb.org/providers/hmis/ . The HMIS Database Manager applies a standard naming convention to all new programs and obtains Data + Evaluation team approval before implementation.

Explanation: New programs must be set up correctly in HMIS before data entry begins to ensure accurate reporting and system-wide consistency. The following steps apply:

- At least 60 days before the anticipated implementation date, the HMIS Agency Administrator completes and submits the electronic HMIS Program Implementation Request Form to the HMIS Database Manager.
- The HMIS Database Manager applies the following naming convention to all new programs: Agency (Abbreviation) – CSB Contract/Program Name Program Type. For example: CSB – Test Program PSH.
- The HMIS Database Manager presents the completed request form and recommended program name to the Data + Evaluation team for review and approval.
- The HMIS Database Manager notifies the HMIS Agency Administrator of approval status at least 30 days before the requested implementation date, allowing the agency at least 30 days to prepare for launch.
- The HMIS Database Manager assists the HMIS Agency Administrator with HMIS implementation as needed.

4.7.2 Making Changes to Existing Programs

Policy: HMIS Agency Administrators must notify the HMIS Database Manager of any programmatic changes that affect data collection, data entry, data quality, or data reporting before implementing those changes in HMIS. Although HMIS Agency Administrators have system access to make program-level changes, all such changes must be coordinated with the HMIS Database Manager in advance.

Explanation: Program changes that require notification include, but are not limited to: expansion of program capacity or scope; changes to funding status or program type; and program termination, deactivation, or discontinuation of HMIS participation. Notification is made via the electronic HMIS Program Implementation Request Form at https://www.csb.org/providers/hmis/ at least 45 days before the proposed implementation date. The HMIS Database Manager circulates the completed form to the Data + Evaluation team for review and comment.

Recommendations and a timeline for assistance are returned to the agency no fewer than 10 business days before the requested implementation date. Pre-coordination ensures that changes are documented, their effect on system-wide reporting is assessed, and any necessary support is arranged before changes go live.

4.7.3 Maintaining an HMIS Program Matrix

Policy: The HMIS Database Manager maintains a complete and current HMIS Program Matrix documenting all programs in the system and their key attributes.

Explanation: The Program Matrix serves as the authoritative index of all programs active and inactive in HMIS. It records each program's status and attributes including funding source, program type, quality assurance participation, and program start and end dates. The HMIS Database Manager updates the Matrix to reflect new program additions and any changes to existing programs, including terminations and deactivations, upon receipt of documentation from the HMIS Agency Administrator and completion of the implementation process.

5. HMIS Privacy Plan

5.1 Purpose and Scope

This HMIS Privacy Plan establishes the privacy policies and procedures governing the collection, use, disclosure, and protection of Protected Personal Information (PPI) entered into the Homeless Management Information System (HMIS) administered by Community Shelter Board (CSB) for the Columbus & Franklin County Continuum of Care (CoC).

This plan is required under 24 CFR 578.7(b)(3) and HUD's HMIS Data Standards and must be reviewed, revised, and approved by the CoC on at least an annual basis. It applies to all Covered Homeless Organizations (CHOs) and their employees, volunteers, affiliates, contractors, and associates who record, use, or process PPI in HMIS.

5.2 Governing Authority and Definitions

5.2.1 Legal and Regulatory Basis

This Privacy Plan is adopted in compliance with the following:

- HUD HMIS Data Standards (most recent version)
- 24 CFR Part 578: CoC Program Interim Rule

- HUD's 2004 HMIS Data and Technical Standards Final Notice (69 FR 45888)
- Applicable federal and state privacy laws

5.2.2 Key Definitions

Protected Personal Information (PPI): Any individually identifying information about a person collected or maintained in HMIS, including name, date of birth, Social Security number, and other data that could be used to identify an individual.

Covered Homeless Organization (CHO): Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, or processes data on clients experiencing homelessness for an HMIS, as defined in the 2004 HMIS Data and Technical Standards Final Notice.

HMIS Lead: Community Shelter Board (CSB), designated by the Columbus & Franklin County CoC as the entity responsible for administering HMIS.

Client: Any individual whose data is collected and maintained in HMIS.

5.3 Client Rights

CSB and all CHOs shall ensure that clients are informed of and afforded the following rights with respect to their personal information in HMIS:

- The right to be notified of the purpose for which PPI is collected and how it will be used.
- The right to refuse or limit disclosure of PPI. Clients who refuse to provide identifying information may still receive services; agencies shall create an 'unnamed' record per CSB procedures.
- The right to review their own HMIS record, upon written request to the agency or CSB.
- The right to request corrections to inaccurate or incomplete data.
- The right to be informed of any mandatory data disclosures required by law.
- The right to file a grievance regarding alleged privacy violations (see Section 5.7).

5.4 Consent and Client Notification

5.4.1 Informed Consent

Before collecting PPI, each CHO must present clients with a Client Acknowledgement for Electronic Data Collection. CHOs shall make reasonable efforts to obtain a signed acknowledgement from each client prior to data entry. If a client declines to sign:

- The CHO must still enter required HMIS data elements provided by the client.
- If a client refuses to provide identifying PPI (name, date of birth, Social Security number), the CHO shall create an 'unnamed' record by contacting the HMIS Database Manager.
- Agencies may implement a more restrictive privacy policy than that mandated by CSB, provided they notify CSB in writing and the policy does not prevent required data collection.

Verbal Consent. Verbal consent may be obtained in lieu of a signed Client Acknowledgement in circumstances where obtaining written consent prior to initial contact is not practical, including contacting the Coordinated Point of Access (CPOA), the Columbus & Franklin County CoC's coordinated entry point, initial contact with a homeless outreach services provider, phone screenings, and street outreach encounters. In these circumstances, the CHO must inform the individual that their information will be entered into HMIS and explain the nature of the data collection. Written consent must be obtained at the individual's first in-person intake appointment.

5.4.2 Privacy Notice

Each CHO shall:

- Post a privacy notice at each intake desk informing clients that a privacy policy is available upon request.
- Maintain a written privacy policy (at minimum, the CSB-mandated policy) covering the collection, use, and maintenance of client PPI.
- Make the privacy policy available on the agency's website, if applicable, and share it with clients upon request.

5.4.3 Educating Clients on Privacy Rights

CHOs are responsible for training intake staff to clearly explain to clients, in plain language: what data is being collected, why it is collected, who can access it, and how clients can request corrections or file a grievance.

5.5 Limits on Data Collection

PPI collected through HMIS must be relevant to the purpose for which it is to be used. CHOs shall collect only the minimum data necessary to:

- Provide direct services to the client,
- Comply with HUD Universal and Program-Specific Data Elements, and
- Support community-level planning and reporting.

CHOs shall not collect PPI for purposes unrelated to the provision of housing and homeless services without explicit client consent. Sensitive categories of information shall be collected only when required by a funding source and shall be subject to heightened protection.

5.6 Data Use, Disclosure, and Sharing

5.6.1 Permitted Uses

PPI in HMIS may be used and disclosed only for the following purposes:

- Verification of eligibility for services
- Entry of records of services provided
- Aggregate reporting to CSB, HUD, and other authorized funders
- Community planning, analysis, and coordination activities authorized by the CoC

- Compliance with applicable law or legal process

5.6.2 Restrictions on Disclosure

CHOs shall:

- Limit access to HMIS data to employees specifically authorized to enter or review data for service-delivery purposes.
- Not share client-level PPI with third parties without written client consent, except as required by law.
- Not use HMIS data for commercial purposes, direct marketing, or solicitation. This restriction does not prohibit CHOs from using aggregate, de-identified data drawn from their own HMIS records to support program advocacy, public awareness, or funding requests to government bodies, funders, or the media, provided no individual client is identified or identifiable.

5.6.3 Inter-Agency Data Sharing

Data sharing between CHOs within the CoC is governed by the inter-agency data sharing policies outlined in Section 4.5 of this document. All inter-agency data sharing arrangements must be documented and comply with HUD data standards.

5.6.4 External Data Requests

Requests for client-level HMIS data from external parties (including researchers, government agencies, and media) must be submitted to the CSB Data + Evaluation team. Requests may be submitted by email to HMIS@CSB.org or through the external data request form available at https://www.csb.org/providers/hmis/ . CSB will evaluate each request against applicable privacy protections and HUD standards before any data is released. Only de-identified or aggregate data will be shared externally unless a legal obligation requires otherwise.

5.7 Grievance Procedures

5.7.1 Client Grievances

A client who believes their privacy rights have been violated may file a grievance with the CHO's designated privacy contact (which may be the HMIS Agency Administrator, a privacy officer, or other staff member designated by the CHO for this purpose) or directly with CSB's HMIS Database Manager. Grievances must be:

- Submitted in writing (in person, by mail, or by email),
- Reviewed by CSB within 30 calendar days of receipt,
- Responded to in writing with findings and, where applicable, corrective action.

5.7.2 CHO Grievances

CHOs with grievances related to privacy policies or practices may follow the CHO Grievance procedures outlined in Section 3.1 of this document.

5.8 CHO Privacy Responsibilities

All CHOs are required to:

- Abide by all federal and state laws and regulations governing privacy of HMIS information.
- Limit HMIS access to trained, authorized, and HMIS-certified staff.
- Ensure each user has a unique username and password; sharing of login credentials is prohibited.
- Complete data entry in secure locations; computers must be equipped with locking screen savers.
- Maintain virus protection and firewall software on all computers used for HMIS access.
- Maintain a written client privacy policy and ensure staff are trained on its requirements.
- Ensure the CHO Executive Director (or designee) accepts responsibility for the accuracy and privacy compliance of all records entered by the agency.
- Report any suspected privacy breach to the HMIS Database Manager within 24 hours of discovery.

6. HMIS Security Plan

6.1 Purpose and Scope

This HMIS Security Plan documents the physical, administrative, and technical safeguards that Community Shelter Board (CSB) and its Covered Homeless Organizations (CHOs) maintain to protect HMIS data from unauthorized access, disclosure, alteration, and destruction.

This plan is required under 24 CFR 578.7(b)(3) and HUD's HMIS Data Standards and must be reviewed, revised, and approved by the Columbus & Franklin County CoC. It applies to all individuals and organizations with access to the Clarity Human Services HMIS platform administered by CSB.

6.2 Governing Authority and Roles

6.2.1 Regulatory Basis

- 24 CFR Part 578, CoC Program Interim Rule
- HUD HMIS Data Standards (most recent version)
- HUD's 2004 HMIS Data and Technical Standards Final Notice
- Applicable federal and state data security laws

6.2.2 Security Responsibilities

Designated HMIS Security Officer. In accordance with HUD HMIS Data Standards and the Columbus and Franklin County CoC Governance Charter, CSB designates one staff member as the HMIS Security Officer responsible for implementing and overseeing this Security Plan.

The HMIS Database Manager serves as the designated HMIS Security Officer for the Columbus and Franklin County CoC. In the event of a vacancy in the HMIS Database Manager position, the Deputy Chief, Housing + Data Systems assumes security officer responsibilities until the position is filled. CSB will notify the CoC Board of any change in the designated HMIS Security Officer within 30 days of the change.
CSB also requires each Covered Homeless Organization to designate an agency-level security contact responsible for enforcing security policies at the agency level. This responsibility is fulfilled by the HMIS Agency Administrator designated under each CHO's HMIS Agency Agreement. CHOs with a designated backup contact are encouraged to assign security responsibilities to that individual as well.

HMIS Database Manager: Serves as CSB's primary security contact. Responsible for monitoring system access, coordinating with BitFocus on security issues, managing user access controls, and leading incident response.

Back-up HMIS Database Manager: Assumes security responsibilities of the HMIS Database Manager in their absence.

Deputy Chief, Housing + Data Systems: Provides supervisory oversight of security functions and is notified of any significant security incidents or breaches.

BitFocus: As CSB's HMIS software vendor and host, BitFocus maintains the central server environment and is responsible for infrastructure-level security controls described in Section 4.

HMIS Agency Administrators (CHOs): Responsible for enforcing security policies at the agency level, including user access management, hardware security, and staff training.

6.3 Central Server and Hosting Security

Clarity Human Services HMIS is maintained and hosted by BitFocus. BitFocus employs a dedicated team of full-time experts who ensure system availability, performance, and security using current industry standards. The HMIS Database Manager serves as the primary liaison between CSB and BitFocus and is responsible for monitoring and tracking security issues at the central database level.
CSB maintains a disaster recovery plan documenting protocols for communicating with staff, the CoC, and CHOs in the event of a significant system disruption or data loss event, as required by the CoC Governance Charter and HUD HMIS Data Standards. The plan is maintained by the HMIS Database Manager and reviewed annually as part of the security review process described in Section 6.4.6. The full Disaster Recovery Plan is incorporated into this document as Section 8. BitFocus maintains documented nightly backup and emergency recovery procedures for the hosted HMIS environment, as described in Section 6.3.2.

6.3.1 Physical Safeguards (BitFocus Data Center)

The BitFocus hosting environment incorporates the following physical security controls:

- Physically secure data center facility with 24/7/365 on-site staffing
- Biometric scanner access controls at facility entry points
- Dual-factor authentication required for physical access to server areas
- Continuously monitored security scanners throughout the facility

6.3.2 Technical Safeguards (BitFocus Infrastructure)

The Clarity HMIS platform incorporates the following technical security controls:

- Documented nightly backup and emergency recovery procedures
- Secure API capability with AES-encrypted traffic
- Unique user authentication required for all system access
- End-to-end data encryption using 2048-bit SSL at rest and during transfer
- Role-based data access controls limiting user access to authorized data only
- Automatic session time-out and account lockout after periods of inactivity
- Password policy enforcement including complexity and expiration requirements
- Concurrent login prevention: simultaneous sessions for a single user are blocked
- Two-factor authentication for system access
- IP allowlisting to restrict access to authorized network locations
- Detailed audit logs capturing all user access and data modification events
- Strong network firewalls protecting the hosted environment
- All HMIS web traffic served over HTTPS (SSL) with 2048-bit encryption or better

6.4 CSB Administrative Safeguards

6.4.1 User Access Management

CSB controls access to HMIS through the following procedures:

- All HMIS users must complete an HMIS User Agreement before being granted access.
- User access is assigned based on role and the principle of least privilege.
- HMIS Agency Administrators are responsible for requesting new user accounts and notifying the HMIS Database Manager promptly when a user's access should be terminated.
- The HMIS Database Manager reviews active user accounts periodically and deactivates accounts for users who have left or changed roles.
- Terminated employees must have HMIS access revoked on the date of termination.

6.4.2 Password Requirements

All HMIS user accounts are subject to the following password standards, enforced by the Clarity platform:

- Passwords must meet minimum complexity requirements (combination of letters, numbers, and special characters).
- Passwords must be changed at regular intervals as configured in the system.

- Users must not share passwords; each user must maintain a unique login credential.
- Password recovery is managed through the Clarity platform's secure recovery process.

Specific password complexity requirements, including minimum character length, required character types, prohibited content, and the 90-day expiration cycle, are documented in Section 3.2 (Passwords) of this document. The requirements in Section 3.2 govern and are incorporated into this Security Plan by reference.

6.4.3 Extracted Data Security

Data extracted from HMIS for reporting or analysis purposes must be handled in accordance with the following:

- Extracted data containing PPI must be stored on password-protected, encrypted devices or systems.
- Extracted data must not be stored on portable media (USB drives, external hard drives) unless encrypted.
- Client-level extracted data must be deleted when no longer needed for the stated purpose.
- Aggregate or de-identified data extracts do not require the same controls but must not be re-identified.

6.4.4 Remote Access

Users accessing HMIS remotely must ensure:

- Access is only through secure, trusted networks or via an approved VPN connection.
- Computers used for remote access meet the hardware and software requirements specified by CSB.
- HMIS is never accessed on public or shared computers (e.g., library terminals, shared workstations).
- Users log out completely after each remote session.

6.4.5 Digital Data Retention

HMIS data is retained in accordance with HUD data standards and applicable law. CSB maintains client-level data for a minimum of seven years following a client's last program activity. Data retention schedules are reviewed by the HMIS Database Manager annually.

6.4.6 Annual Security Review

The HMIS Database Manager, in the designated role of HMIS Security Officer, conducts a comprehensive annual security review each fiscal year to assess implementation of the security requirements contained in this plan for both CSB and all participating CHOs. The annual review includes:

- Assessment of CSB's internal compliance with each administrative safeguard in Section 6.4, including user access management, password policy enforcement, extracted data handling, and remote access controls.
- Review of CHO-level compliance with Section 6.5 security responsibilities, conducted through the annual HMIS monitoring process, HMIS Agency Administrator communications, and available system audit data.
- Review of the BitFocus security posture, including any updates to physical or technical safeguards described in Section 6.3, based on information provided by BitFocus through the annual contract review or vendor security reporting.
- Assessment of any security incidents or data breaches that occurred during the prior fiscal year, including a review of response actions taken and whether corrective measures remain adequate.
- Review and update of this Security Plan to reflect any changes in HUD guidance, CoC priorities, BitFocus infrastructure, or identified security risks.

Findings from the annual security review are documented in a written summary retained by the HMIS Database Manager. Material findings are reported to the Deputy Chief, Housing + Data Systems and, where relevant, to the CoC Board as part of the annual governance plan review process. The annual review is completed prior to the start of each fiscal year to inform the CoC's plan approval process under Section 6.8.

6.5 CHO Security Responsibilities

All Covered Homeless Organizations are required to implement and maintain the following security measures at the agency level:

- Acquire and maintain computers, software, and network connections adequate for secure HMIS access.
- Ensure all computers used for HMIS data entry are equipped with locking screen savers.
- Install and maintain current virus protection software with automatic updates on all HMIS workstations.
- Implement individual or network firewalls on all computers used for HMIS access.
- Conduct data entry only in secure, private locations where unauthorized individuals cannot view screen content.
- Ensure each HMIS user has a unique username and password; sharing of login credentials is strictly prohibited.
- Report any suspected unauthorized access, data breach, or loss of a device containing HMIS data to the HMIS Database Manager within 24 hours of discovery.
- Train all HMIS users on security policies before granting system access and annually thereafter.

6.6 Data Breach Response

6.6.1 Definition

A data breach is any incident in which PPI maintained in or extracted from HMIS is accessed, disclosed, altered, or destroyed without authorization. This includes loss of a device containing extracted HMIS data, unauthorized system access, and inadvertent disclosure to an unauthorized party.

6.6.2 Reporting

- CHOs must report any known or suspected breach to the HMIS Database Manager within 24 hours of discovery.
- The HMIS Database Manager will notify the Deputy Chief, Housing + Data Systems, and the CSB CEO within 24 hours of receiving a breach report.
- CSB will notify BitFocus and coordinate a technical assessment of the incident.

6.6.3 Response Steps

- Contain: Take immediate steps to prevent further unauthorized access or disclosure.
- Assess: Determine the nature and scope of the breach, including what data was affected and how many clients may be impacted.
- Notify: Notify affected clients and any required agencies or regulators in accordance with applicable law and HUD guidance.
- Remediate: Implement corrective actions to address the root cause of the breach.
- Document: Prepare a written incident report summarizing the breach, response actions, and any corrective measures. Retain for at least seven years.

6.7 Multiple Log-On Restriction

HMIS users are not permitted to maintain multiple simultaneous login sessions. The Clarity platform enforces concurrent login prevention. If a user suspects their credentials have been used by another individual, they must immediately report this to their HMIS Agency Administrator and the HMIS Database Manager.

7. HMIS Data Quality Plan

7.1 Purpose and Scope

This HMIS Data Quality Plan establishes the framework, benchmarks, roles, and procedures by which Community Shelter Board (CSB) and the Columbus & Franklin County Continuum of Care (CoC) ensure the accuracy, completeness, timeliness, and consistency of data entered into HMIS by all Covered Homeless Organizations (CHOs).

This plan is required under 24 CFR 578.7(b)(3) and HUD's Data Quality Management Program guidance, and must be reviewed, revised, and approved by the CoC. It applies to all CHOs participating in HMIS, regardless of funding source.

High-quality HMIS data is essential for: accurate community-level reporting to HUD (including the Point-in-Time Count, Housing Inventory Count, System Performance Measures, and Longitudinal Systems Analysis (LSA)); equitable prioritization of individuals experiencing homelessness through Coordinated Entry; and data-informed funding and resource allocation decisions by CSB and its partners.

7.2 Governing Authority and Definitions

7.2.1 Regulatory Basis

- 24 CFR Part 578: CoC Program Interim Rule
- HUD HMIS Data Standards (most recent version)
- HUD Data Quality Management Program (DQMP) guidance
- HUD CoC Data Quality Brief
- HUD SNAPS Data TA Strategy to Improve Data and Performance

7.2.2 Data Quality Indicators

Completeness: The degree to which all required data elements are known and documented for each client record, bed unit, and participating agency.

Accuracy: The degree to which data reflects the client's actual situation and the services provided. Accuracy depends on comprehensive staff training and adherence to HUD data collection protocols.

Timeliness: The length of time between when client data is collected and when it is entered into HMIS. Timely data entry supports real-time decision-making and accurate reporting.

Consistency: The degree to which data is collected, entered, and maintained in a uniform manner across all CHOs and over time.

7.3 Roles and Responsibilities

7.3.1 Community Shelter Board (CSB) / HMIS Lead

- Develop, maintain, and update this Data Quality Plan.
- Submit the plan to the CoC for annual review and approval.
- Monitor data quality across all CHOs through regular reporting and site visits.
- Provide training, technical assistance, and resources to CHOs to support data quality improvement.
- Apply encouragements and enforcements as outlined in Section 7.8 of this document.
- Communicate data quality performance results to the CoC, CHOs, and other stakeholders.

7.3.2 Columbus & Franklin County CoC

- Review, revise, and approve this Data Quality Plan at least annually.

- Support consistent CHO participation in HMIS as a condition of CoC funding.
- Integrate data quality performance into CoC funding prioritization decisions.

7.3.3 HMIS Agency Administrators (CHOs)

- Implement and enforce this Data Quality Plan at the agency level.
- Ensure all agency HMIS users complete required training and certification before system access.
- Perform routine quality assurance procedures per the schedules in Section 7.5 of this document.
- Promptly correct data errors and inaccuracies identified through QA review.
- Report data quality concerns and challenges to the HMIS Database Manager.

7.3.4 HMIS End Users

- Enter client data accurately and completely at the time of service.
- Follow CSB's data collection protocols and HUD data standards.
- Participate in required HMIS training and certification.

7.4 Data Quality Benchmarks

7.4.1 Completeness Standards

Missing, unknown, or 'data not collected' responses for required data elements must remain below the following thresholds:

- Missing/unknown data in required fields: less than 5% per month per project.
- Client profile duplicate rate: less than 5% of clients served per month or per quarter.
- Dates of birth and Social Security numbers are high-priority completion fields. High rates of missing dates of birth result in unclassifiable households in the LSA; high rates of missing Social Security numbers undermine system-wide deduplication. These fields require additional attention beyond the general 5% missing data threshold.
- Bed utilization: all beds within the CoC's geographic area should be recorded in HMIS. Per HUD LSA guidance, inventory with below 65% utilization or above 105% utilization will generate a data quality flag requiring review.
- Agency coverage: all CHOs funded by the CoC Program, CoC Builds, ESG, YHDP, or other HUD-designated programs must participate in HMIS. All residential continuum projects within the Columbus & Franklin County CoC geographic area must be recorded in HMIS regardless of their participation status, per HUD FY2026 HMIS Data Standards.

7.4.2 Accuracy Standards

Data must accurately reflect client information recorded in the agency's files and known facts about the client. Common accuracy errors that CHOs must monitor and correct include:

- Multiple open entries into the same project type for the same client
- No defined head of household, or multiple heads of household, in a household record
- Exit dates that do not reflect the client's actual physical exit from the program
- Data incompatible with the project type (e.g., a family enrolled in a single-adult program)
- Demographic data that does not match verified intake documentation
- Overlapping enrollments must not exceed 1% per project per reporting period. Above this threshold, HUD LSA generates an error flag requiring data cleaning. Below this threshold, a warning flag is generated and data should still be reviewed for accuracy.
- Each household record must have exactly one head of household designated for the full duration of the household's enrollment. If the designated head of household exits while other members remain enrolled, another member must be immediately designated as the new head of household, retroactive to the beginning of the enrollment.
- Clients in Emergency Shelter Night-by-Night (ES-NbN) projects must be exited no later than 90 days after their last recorded bed night. ES-NbN projects should use auto-exit functionality where available, or manually exit clients at the 90-day mark with an exit date backdated to the day after the last bed night. HUD LSA flags clients with exit dates extending 90 or more days past their most recent bed night.
- Clients in Rapid Re-Housing (RRH) and Permanent Supportive Housing (PSH) projects who exit to permanent housing must have a Housing Move-In Date recorded. Per HUD FY2022 Data Standards, this requirement applies to all clients exiting after October 1, 2021. The Housing Move-In Date is the first night the client slept in the unit, which may differ from the lease signing date.

7.4.3 Timeliness Standards

Data entry must meet the following timeliness requirements:

- Emergency Shelter Projects: Clients who stayed in shelter during the previous 24-hour period must be entered into HMIS by 9:00 a.m. the following day. Complete and accurate data for the month must be corrected in HMIS by the fourth (4th) business day of the following month.
- All Other Projects: Data for all persons served must be entered into HMIS within 48 hours of the service or contact date. Complete and accurate data for the month must be corrected in HMIS by the fourth (4th) business day of the following month.

7.4.4 Consistency Standards

CSB expects data to be collected and entered consistently across all CHOs and over time. Consistency benchmarks include:

- All staff entering data into the same project type should use the same data collection instruments and entry workflows.
- HMIS entries should reflect the same service definitions used in the agency's paper or electronic client files.
- Agencies should not change data collection practices without notifying the HMIS Database Manager.

7.5 Agency-Level QA Procedures

HMIS Agency Administrators must implement the following minimum QA procedures. Frequency varies by agency size:

QA Task	< 200 Households/yr	> 200 Households/yr
Run QA report for each project. Review open cases; exit cases that are closed; enter cases that are open.	Monthly	Weekly
Review QA report for missing data in required fields. Correct to keep missing data < 5%.	Monthly	Weekly
Run Client Duplicate report. Notify HMIS Database Manager of any duplicates found.	Monthly	Monthly
Pull 10% of paper files and compare to HMIS records for accuracy.	Monthly	Monthly
Review and correct data incompatible with the project type.	Monthly	Monthly

7.6 CSB Monitoring and Reporting

7.6.1 System-Level Monitoring

The HMIS Database Manager conducts regular data quality monitoring across all CHOs, including:

- Monthly review of data quality reports for each CHO and project.
- Quarterly reporting to the Data + Evaluation team on system-wide data quality performance.
- Annual reporting to the CoC summarizing data quality status across the system.
- Submission of required HUD reports (LSA, SPMs, PIT, HIC) using HMIS data.

7.6.2 Site Monitoring Visits

CSB may conduct data quality monitoring visits with individual CHOs, either on a scheduled basis or in response to identified data quality concerns. Monitoring visits may include:

- Review of agency QA procedures and documentation
- Comparison of paper/electronic client files with HMIS records
- Observation of data entry practices
- Staff interviews regarding data collection workflows

Findings from monitoring visits will be documented and shared with the HMIS Agency Administrator. CHOs with significant findings will be required to submit a written Data Quality Improvement Plan within 30 days.

7.7 Enforceable Agreements

Data quality expectations are incorporated into binding agreements between CSB and each CHO, including:

- HMIS Agency Agreement: requires compliance with CSB data quality standards as a condition of HMIS access for all participating organizations.
- Master Provider Agreement (for CSB-funded Partner Agencies): the MPA references HMIS data quality requirements as a contractual obligation, in addition to this Agreement.
- HMIS User Agreement: each individual user commits to accurate, timely, and complete data entry.

7.8 Encouragements and Enforcements

7.8.1 Encouragements

CSB will recognize and support CHOs that demonstrate strong data quality performance through:

- Public recognition of high-performing agencies in CoC communications
- Priority consideration for technical assistance and training resources
- Data quality performance factored favorably in relevant CSB reporting and evaluation activities

7.8.2 Corrective Actions

When a CHO's data quality falls below established benchmarks, CSB will:

- Issue a written notice to the HMIS Agency Administrator identifying the deficiency and required corrective action.
- Require submission of a written Data Quality Improvement Plan within 30 days.
- Provide targeted training and technical assistance to support improvement.
- Conduct a follow-up monitoring review within 60 days.

For persistent or serious data quality failures, CSB may:

- Notify the CHO Executive Director and escalate to CSB leadership.
- Place conditions on the CHO's HMIS access or participation.

- For CSB-funded agencies, address data quality failures in the context of the broader funding relationship.

8. HMIS Disaster Recovery Plan

8.1 Purpose and Scope

This HMIS Disaster Recovery Plan establishes the procedures Community Shelter Board (CSB) will follow to maintain and restore access to the Homeless Management Information System (HMIS) in the event of an unplanned disruption, system outage, or data loss event. It documents communication protocols for staff, the Columbus & Franklin County Continuum of Care (CoC), and Covered Homeless Organizations (CHOs), and assigns recovery responsibilities.

This plan is required by the Columbus & Franklin County CoC Governance Charter and HUD's HMIS Data Standards. It complements and operates alongside the HMIS Security Plan (Section 6 of the HMIS Policies and Procedures) and BitFocus' infrastructure-level backup and recovery procedures. It applies to all disruptions affecting the availability or integrity of HMIS data or system access, regardless of cause.

This plan does not replace BitFocus' contractual obligations for system recovery, nor does it govern data breach response, which is addressed separately in the HMIS Security Plan, Section 6.6.

8.2 Regulatory Basis

- Columbus & Franklin County CoC HMIS Governance Charter (FY2027)
- HUD HMIS Data Standards (FY2026, effective October 1, 2025)
- 24 CFR Part 578, CoC Program Interim Rule
- HUD's 2004 HMIS Data and Technical Standards Final Notice
- CSB–BitFocus Software and Hosting Agreement

8.3 Roles and Responsibilities

The following individuals hold primary responsibility for disaster recovery activities. Contact information for all roles is maintained by the HMIS Database Manager and updated whenever personnel changes occur.

Role	Responsibility	Backup
HMIS Database Manager	Primary recovery coordinator. Activates this plan, leads all communications, coordinates with BitFocus, and directs CHO notifications.	Back-up HMIS Database Manager
Back-up HMIS Database Manager	Assumes all HMIS Database Manager recovery	Deputy Chief, Housing + Data Systems

Role	Responsibility	Backup
	responsibilities when the primary is unavailable.	
Deputy Chief, Housing + Data Systems	Supervisory oversight of recovery operations. Receives all significant incident notifications. Escalates to CSB President + CEO as warranted.	CSB President + CEO
CSB President + CEO	Final authority on extended outages, external communications, and decisions requiring executive action.	—
BitFocus	Infrastructure-level recovery: server restoration, data backup retrieval, platform availability. Primary contact: BitFocus Support (support@bitfocus.com).	—
HMIS Agency Administrators (CHOs)	Notify the HMIS Database Manager of access issues, implement interim data collection procedures at the agency level, and communicate with their agency's staff and clients.	CHO Backup Contact

8.4 Disruption Types and Severity Levels

This plan addresses the following categories of disruption. Severity level determines the communication and recovery response required.

Level	Type	Examples	Initial Response Window
1: Minor	Brief planned or unplanned outage	Scheduled maintenance, short platform slowdown (< 2 hours)	Monitor; notify CHOs if unplanned and > 30 minutes

Level	Type	Examples	Initial Response Window
2: Moderate	Extended unplanned outage	Platform unavailable 2–24 hours; access errors for multiple CHOs	Activate this plan; notify all CHOs within 2 hours
3: Significant	Extended outage or partial data loss	Platform unavailable > 24 hours; data corruption in one or more programs	Activate this plan; notify all CHOs within 1 hour; notify CoC Board
4: Critical	Full system failure or major data loss	Complete platform unavailability; loss of significant client records; disaster affecting BitFocus infrastructure	Activate this plan immediately; notify all CHOs within 1 hour; notify CoC Board; notify HUD if data loss is unrecoverable

8.5 Detection and Activation

8.5.1 Detection

A disruption may be detected by any of the following:

- The HMIS Database Manager observing system unavailability or degraded performance during routine monitoring
- An HMIS Agency Administrator or end user reporting access issues to HMIS@CSB.org
- A notification from BitFocus of a planned or unplanned outage
- An automated system alert from the Clarity HMIS platform

Any CHO user who cannot access HMIS or observes unusual system behavior must report the issue to their HMIS Agency Administrator immediately. The HMIS Agency Administrator must notify the HMIS Database Manager at HMIS@CSB.org or by phone.

8.5.2 Activation

The HMIS Database Manager activates this plan when a disruption is confirmed at Level 2 or above, or when any disruption is of unknown severity and cannot be resolved within 30 minutes through normal support channels. To activate:

- Confirm the disruption by attempting to access HMIS and contacting BitFocus Support.
- Assign a severity level based on the Disruption Types table in Section 4.
- Notify the Deputy Chief, Housing + Data Systems of the activation and assigned severity level.
- Begin stakeholder communications per Section 6.

- Document the time, nature, and assigned severity of the disruption in the Incident Log (Section 9).

8.6 Communication Protocols

8.6.1 Internal CSB Communications

Severity	Notify	Timing
Level 1	No internal escalation required unless duration exceeds 2 hours	N/A
Level 2	Deputy Chief, Housing + Data Systems	Within 1 hour of activation
Level 3	Deputy Chief, Housing + Data Systems; CSB President + CEO	Within 1 hour of activation
Level 4	Deputy Chief, Housing + Data Systems; CSB President + CEO; CSB Board (at President + CEO's discretion)	Immediately upon activation

8.6.2 BitFocus Communications

The HMIS Database Manager is the sole point of contact with BitFocus during a recovery event. The HMIS Database Manager will:

- Contact BitFocus Support immediately upon confirming a Level 2 or higher disruption.
- Obtain an estimated time to restoration (ETR) and share with internal CSB leadership and HMIS Agency Administrators.
- Request a written incident summary from BitFocus upon resolution for inclusion in the Incident Log.
- For Level 4 events involving data loss, request a full accounting of what data was affected, the scope of loss, and the recovery actions taken.

BitFocus Support contact: support@bitfocus.com | Available 24/7 for critical outages. Non-critical support requests are addressed during business hours.

8.6.3 CHO Communications

The HMIS Database Manager is responsible for notifying all HMIS Agency Administrators of any unplanned disruption. Notification channels are email to all active HMIS Agency Administrators (using the distribution list maintained by the HMIS Database Manager) and,

for Level 3 or 4 events, direct phone contact with HMIS Agency Administrators of high-volume or time-sensitive programs (e.g., emergency shelters).

Severity	CHO Notification Content
Level 1	Optional. If notified: brief description of issue, estimated duration, and whether CHOs are affected.
Level 2	Email to all HMIS Agency Administrators within 2 hours of activation. Include: nature of the disruption, estimated duration (if known), interim data collection guidance (see Section 7), and expected next update time.
Level 3	Email and direct phone contact with high-volume/time-sensitive agencies within 1 hour. Include all Level 2 content plus guidance on client service continuity and any data integrity concerns.
Level 4	Email and direct phone contact within 1 hour. Include: full description of the event, what data may be affected, interim procedures, and a commitment to a written update within 24 hours.

8.6.4 CoC Communications

The Deputy Chief, Housing + Data Systems notifies the CSB President + CEO of any Level 3 or Level 4 event within 24 hours of activation. Notification includes the nature of the disruption, actions taken, and estimated impact on CoC-level reporting or HUD submission deadlines. A written incident summary is provided to the CoC Board following resolution.

8.6.5 HUD Communications

CSB will notify HUD's local CPD Field Office if a Level 4 event results in unrecoverable data loss affecting HUD-required reporting, including the Point-in-Time Count, Housing Inventory Count, LSA, APR, or System Performance Measures. The HMIS Database Manager drafts the notification; the CSB President + CEO approves before transmission. CSB will coordinate with the CPD Field Office to determine whether a report deadline extension or data substitution methodology is warranted.

8.7 Interim Data Collection Procedures

During any outage at Level 2 or above, CHOs must continue to document client interactions and services. Data entered after HMIS is restored must be backdated to the actual date of service.

8.7.1 Emergency Shelter Programs

Emergency shelter programs must maintain a manual nightly count of individuals served during any period of HMIS unavailability. At minimum, record:

- Date of service

- Number of beds occupied (total; breakdown by household type if possible)
- Names of individuals served, if known, for retroactive HMIS entry

Shelter programs must enter all manually collected data into HMIS within 24 hours of system restoration, backdated to the actual nights of service.

8.7.2 All Other Programs

All other CHOs should use agency intake forms, case management records, or paper-based alternatives to document client interactions during the outage. Required data elements are listed in the HMIS Local Data Dictionary. CHOs must enter all manually collected data into HMIS within 48 hours of system restoration, backdated to the actual service dates.

8.7.3 Data Entry After Restoration

Upon HMIS restoration, the HMIS Database Manager will issue a notice to all HMIS Agency Administrators confirming that the system is available and providing any specific guidance on retroactive data entry. HMIS Agency Administrators are responsible for ensuring all missed data is entered and for notifying the HMIS Database Manager when retroactive entry is complete.

8.8 Recovery Procedures

8.8.1 BitFocus-Managed Recovery (Primary)

Because Clarity Human Services HMIS is hosted and maintained by BitFocus, the primary recovery mechanism for any server-level or platform-level disruption is BitFocus' own incident response and recovery procedures, which include:

- Nightly automated backup of all HMIS data to geographically redundant storage
- Documented emergency recovery procedures with defined recovery time and recovery point objectives
- 24/7/365 infrastructure monitoring by BitFocus operations staff
- Escalation procedures for major outages including direct executive engagement

CSB's role during a BitFocus-managed recovery is to communicate with stakeholders (Section 6), implement interim data collection (Section 7), and monitor the recovery timeline. CSB does not independently manage server-level recovery.

8.8.2 CSB Administrative Recovery

CSB is responsible for the following recovery actions regardless of whether the disruption originates at the platform level or locally:

- **User access verification:** Following restoration, confirm that all user accounts are accessible and access levels are correct. Report any anomalies to BitFocus immediately.

- **Data integrity check:** Review data entered immediately before and after the disruption for any anomalies, gaps, or duplicate records. Run standard QA reports within 5 business days of restoration.
- **Retroactive entry verification:** Confirm with HMIS Agency Administrators that all missed data has been entered and backdated. Document completion in the Incident Log.
- **Reporting impact assessment:** Assess whether the disruption affects any pending HUD report submissions and take corrective action, including requesting deadline extensions if necessary.

8.8.3 Recovery from Data Loss

If BitFocus confirms that data has been permanently lost, the HMIS Database Manager will:

- Obtain a written report from BitFocus documenting the scope of loss (date range, affected programs, number of records).
- Notify the Deputy Chief, Housing + Data Systems and CSB President + CEO.
- Notify affected CHOs, identifying which programs and date ranges are affected.
- Work with affected CHOs to reconstruct lost data from agency records, to the extent possible.
- Document all reconstruction efforts and any data that could not be recovered.
- Notify HUD's CPD Field Office if the loss affects required HUD reporting (see Section 6.5).

8.9 Incident Log

The HMIS Database Manager maintains a written Incident Log for every disruption at Level 2 or above. The log is retained for a minimum of seven years and is reviewed as part of the annual security review process described in Section 6.4.6 of the HMIS Policies and Procedures.
Each log entry must include:

- Date and time the disruption was detected
- Date and time this plan was activated (if applicable)
- Assigned severity level
- Description of the disruption
- Actions taken and by whom
- Timeline of stakeholder communications
- Date and time HMIS was restored
- Any data loss or integrity issues identified
- Retroactive data entry status
- Written incident summary received from BitFocus (attached)
- Any HUD notifications made
- Lessons learned and any recommended changes to this plan

9. Document Control

9.1 Plan Review and Approval

This HMIS Policies and Procedures document, including all incorporated plans (Sections 5–8), shall be reviewed annually by the HMIS Database Manager and submitted to the Columbus & Franklin County CoC for review, revision, and formal approval, as required by 24 CFR 578.7(b)(3). The document shall also be updated in response to significant changes in HUD guidance, CoC priorities, applicable law, or HMIS operations.

9.2 Document Ownership

Plan Owner: HMIS Database Manager, Community Shelter Board

9.3 Supersedes

This document supersedes the following prior instruments:

- Any prior HMIS privacy provisions contained within the HMIS Policies and Procedures: Columbus & Franklin County CoC (Section 5)
- Safeguards and Technical Safeguards provisions previously contained in Section 2 of the HMIS Policies and Procedures Manual (Section 6)
- Client Tracking & QA Standards (Section A) of the CSB HMIS Data Dictionary (FY25), to the extent that document served as the CoC's Data Quality Plan (Section 7)
- No prior standalone document exists for the Disaster Recovery Plan; this is its first edition (Section 8)

9.4 Related Documents

- HMIS Governance Charter, Columbus & Franklin County CoC (FY2027)
- HMIS Local Data Dictionary, Columbus & Franklin County CoC
- HUD HMIS Data Standards (most recent version)
- CSB Privacy and Data Security Policy (csb.org)
- CSB–BitFocus Software and Hosting Agreement