

**ERIE COUNTY
CONTINUUM OF CARE
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
MANAGED BY: THE ERIE UNITED METHODIST ALLIANCE
POLICY AND PROCEDURE MANUAL**

Erie County PA Homeless Management Information (HMIS-Erie) System Policy and Procedure Manual lists local procedures for operating the HMIS. It documents specific expectations regarding the use of the system and procedures that should be followed regarding routine and occasional functions.

SECTION 1: Federal Operating Procedures

Erie County Continuum of Care (ECCoC) adheres first and foremost to policies and procedures outlined in the Department of Housing and Urban Development HMIS Data and Technical Standards Final Notice 2009.

SECTION 2: Contractual Requirements and Roles

ECCoC Contract Requirements: Erie United Methodist Alliance, in its role as the HMIS Lead Agency for Erie County Dept. of Human Services office of MH/MR (ECDHS-MH/MR), agrees to provide the necessary equipment and staff to operate and maintain the centralized HMIS database site. This includes required licenses for software¹ and direct technical assistance to sites who serve homeless populations, with regard to the HMIS application. This applies to all Contributory HMIS Organizations (CHO) that Erie County CoC is currently funded to serve.

ECCoC New Sites Requirements: Any CHO that ECCoC does not receive alternate funding for but does want to participate must assume the costs of requisite licenses and cost share of central resources.

HMIS Project Team: HMIS Lead utilizes the HMIS Project Team to provide general oversight and guidance to the project.

HMIS-Erie Server Management: Management of an HMIS requires several divergent skill sets. The HMIS-Erie project has identified the following roles to provide the best, most efficient service to our stakeholders:

- Project Manager
- Requirement Analyst
- Technical Support Specialist
- Trainer
- Application Administrator

The project also designates the roles of every participating user in order to prevent any confusion around responsibilities and privileges. Each role must be filled in order for the Agency to begin working with the project: Participating Agency Executive Director, and User.

1-Due to budget constraints, CHO's will be limited to a maximum of two user licenses per organization. Exceptions will be made as necessary based on demonstrated need. Any CHO wishing to purchase additional user licenses may contact the HMIS-Erie Administrator.

SECTION 3: Participation Requirements

Participation Requirements: For most efficient utilization of the services provided by HMIS Lead, several steps must be completed at the Agency level before implementation can begin. Steps include:

- High Speed Internet Connectivity (DSL or Broadband);
- Identification of a Site Technical Administrator to serve as primary contact;
- Signed Participation Agreement contract; and
- Establishing client consent procedures and interview protocols.

Central Server Requirements: This section covers the exact equipment, staffing, and procedures that the HMIS-Lead staff is responsible for. Focused on security, the areas are:

- Hardware Physical Security
- Software Security
- Network security
- Client database security

Implementation Requirements: Agencies must generate documents that cover each of the following areas in order for implementation to begin.

➤ Participation Agreement: Each participating Agency must agree to the requirements set forth in the Participation Agreement, which must be signed by a duly authorized Agency representative and returned to the Agency's HMIS Lead. Each Agency must complete the Provider Form.

➤ Privacy Notice to Consumers: Each participating Agency must use a Privacy Notice. HMIS Lead will provide an HMIS Privacy Notice to each participating Agency for each Agency to adapt to their needs. Each participating Agency must provide a copy of the adapted Privacy Notice to ECDHS-MH/MR. If the participating Agency is a HIPAA covered entity, the Agency may continue to use its' own Privacy Notice; however ECDHS-MH/MR must have copy of it on file.

➤ Privacy Posting: Each participating Agency must post the Privacy Summary in a conspicuous place at each Provider site. ECDHS-MH/MR will provide the Privacy Summary, which is a summary of the Privacy Notice.

➤ Data Collection Commitment: Participation in the HMIS-Erie project requires that all participating Providers collect minimum universal and program specific data elements on all consenting clients.

➤ Information Security Protocols: Internal policies must be developed at each site to establish a process for the violation of any of ECDHS-MH/MR information security protocols.

➤ Implementation Connectivity: Once implementation has begun each site agrees to maintain connectivity in order to continue project participation.

➤ Maintenance of Onsite Computer Equipment: Each Agency agrees to maintain its computer equipment in order to continue project participation.

➤ Policy Update Schedule: HMIS Lead will provide the HMIS Policy and Procedures Manual to each participating Agency. This manual will be updated periodically.

SECTION 4: Training

HMIS Application Training: HMIS Lead provides ongoing training on all relevant aspects of system operation for the duration of the project. Training modules are developed based on skill

level and type of access to the system. Each user of the system is required to complete the application training, as well as HIPAA training, in order to begin using the system.

HIPAA Training: Each participating Agency is responsible for scheduling participating in HIPAA training and certifying that their users are trained. A HIPAA training verification will be required for all new users at the time they attend the HMIS Application training or within 90 days of an on site training.

Scheduled Training Delivery: HMIS Lead provides group user training annually while individual user training will be scheduled on an as needed basis.

HMIS Training Materials: All training documentation will be available on the HMIS page of the HMIS Lead's website, which is <http://www.euma-erie.org/hmis.php>.

HIPAA Training Materials: For HIPAA training and materials contact Robin Dowling at Stairways 814-878-2177.

SECTION 5: User, Location, Physical and Data Access

Access Privileges to System Software: Access to system resources will only be granted to Agency staff that need access in order to perform their job. Users must complete the HMIS User Agreement form, in order to request access privileges. All applicable licensing restrictions apply.

Access Levels for System Users: Each user of the system will be assigned an account that grants access to specific system resources that they require. A model of least-privilege is used; no user will be granted more than the least amount of privilege needed to perform their job.

System Access Deactivation: Participating Agency duly authorized Agency representative will complete the HMIS User Deactivation form within one business day when there is a change in a user's job role or the user is no longer employed by the Agency.

Access to Data: All data collected by the HMIS-Erie project is categorized. Access to datasets, types of data, and all HMIS-Erie data releases is governed by policies developed by the HMIS Project Team.

Access to Client Paper Records: All users of the system must not have greater access to client information through the system than is accessible in the agencies paper files.

Physical Access Control: All equipment or media containing HMIS-Erie data must be physically controlled at the Agency site. Protections and destruction policies vary depending on the type of data and media.

Logical Access: Access to system resources must be limited to authorized users for authorized transactions.

Unique User ID and Password: Each user of the system must be individually and uniquely identified. Identification will be verified through a password.

Right to Deny User and Participating Agencies' Access: HMIS Lead retains the right to suspend or revoke the access of any Agency or individual to the system for consistent or egregious violation of ECCoC policies.

Data Access Control: Access to the system must be audited. All audits may be reviewed regularly.

Auditing - Monitoring, Violations and Exceptions: HMIS Lead considers any exception to stated DTS Computer Security Guideline policies a violation of those policies that must be investigated.

Auditing – Data Logs: HMIS Lead will maintain logs of all actions taken by users. Logs may include operating system logs, database, and firewall logs. All logs may be reviewed regularly.

Data Assessment and Access: All data associated with the HMIS-Erie project is categorized. Access to data is restricted based on the content of the data. Reproduction, distribution, and destruction of data are based on the content of the data.

Data Integrity Controls: Access to the production data is restricted to authorized users only. Each user that has access to production data is contracted to not falsely alter or impact data in any way. If the Agency receives information that necessitates a client's information be entirely removed from the HMIS, the Agency will complete the Client Delete Request form.

Local Data Storage: If agencies choose to store local copies of data they are required to develop policies and procedures on how data is generated, stored, and destroyed.

Transmission of Client Level Data: All authorized users agree to transmit any client level data securely.

Data Accuracy: There are many aspects to data quality, such as validity, completeness, consistency, coverage, accuracy, and timeliness. Each of these aspects is defined in detail in the HMIS Data Quality Standards.

SECTION 6: Technical Support and System Availability

Planned Technical Support: HMIS Lead offers technical support to all participating agencies. Support services include training, implementation support, report writing support, and process troubleshooting.

Participating Agency Technical Service Request: Service requests from participating agencies may originate from any authorized user either by contacting the HMIS Administrator or sending a request to the HMIS email account (hmis@euma-erie.org).

Availability – Hours of System Operation: The system is available to users 24 hours a day, except during routine system maintenance, scheduled system upgrades, and unexpected system failures.

Availability – HMIS-Erie: HMIS Lead staff are available from 8:00 AM to 4:00 PM on Monday to Friday (with the exclusion of holidays) to respond to service requests.

Availability – Planned Interruption to Service: Participating agencies will be notified of planned interruptions to service one week prior to the interruption.

Availability –Unplanned Interruption to Service: In the event of an unplanned interruption to service HMIS Lead staff will immediately notify all authorized users ASAP after system failure.

SECTION 7: Stages of Implementation

Implementation – Stage 1: Start-up and Initial Training: Implementation begins with stage 1. To enter stage 1 an Agency must complete all requisite paperwork and have user accounts created on the system.

Implementation – Stage 2: Data Entry Begins: To enter stage 2 an Agency must begin entering data on their client population.

SECTION 8: Stages of Completion

One week prior to an Agency and/or Provider contract termination, the HMIS Administrator will notify the Agency and/or Provider to exit all clients from the HMIS application. Upon the first business day of the contract termination, the HMIS Administrator will deactivate all user accounts associated with the Agency and/or Provider.

SECTION 9: Encryption Management

Encryption General: All potentially identifying information is encrypted in the database. Encryption prevents unauthorized personnel from accessing confidential information for any reason.

SECTION 10: Data Release Protocols

Data Release Authorization and Distribution: ECCoC does release data in the process of generating reports. ECCoC will only release de-identified aggregate data.

Right to Deny Access to Client Identified Information: ECCoC does not release client identified information to any third party. Court orders for information will be forwarded to the ECDHS-MH/MR Housing Specialist for review. Pursuant to policy no release will occur unless the party obtains the written release of every client within the database prior to receiving the database.

Right to Deny Access to Aggregate Information: HMIS Lead retains the right to deny access to aggregate level data. Pursuant to policy any interested party must submit a request for data to the HMIS Project Team. All requests are reviewed by the HMIS Project Team.