Rhode Island Continuum of Care

Homeless Management Information System (HMIS) Policies and Procedures

Rhode Island Coalition for the Homeless

Edited: September 6, 2018

Table of Contents

1. Introduction

a. Overview

The Rhode Island Homeless Management Information System (HMIS) is a web-based database that is used by homeless service providers across Rhode Island to record and store client-level information to coordinate care and better understand the numbers, characteristics, and needs of persons experiencing homelessness and those at-risk of homelessness. Mediware Information Systems, Inc. administers the central server and provides the HMIS software, ServicePoint. The Rhode Island Coalition for the Homeless is the HMIS Lead Agency and Administrator, managing the system, including, but not limited to managing user licensing, training, data analytics, technical assistance, and compliance. Specific information about governance about HMIS operations can be found in the Rhode Island Continuum of Care (RICOC) Governance Charter.

HMIS enables programs to measure the effectiveness of their interventions, share information between service providers for case coordination, and facilitate longitudinal analysis of service needs and gaps. Guidance for the implementation of Rhode Island's HMIS is provided by Rhode Island's Continuum of Care (CoC) and its subcommittees including the HMIS Steering and System Performance Measures (SysPM) Committees.

This document provides the policy guidelines and standards that govern HMIS operations, as executed by the HMIS Lead Agency and also describes the responsibilities of Participating Agencies and users. It was approved by the RICoC on September 6, 2018 and replaces all earlier documents.

b. Federal HMIS Policies

In addition to the Rhode Island HMIS Policies contained herein, our HMIS must also comply with federal HMIS requirements. These requirements are detailed in a suite of HMIS Data Standard resources, an overview of which is provided below:

Manual Name & Link	Intended Audience	Contents
HMIS Data Standards Dictionary	HMIS Vendors & HMIS Lead Agencies	The manual provides the detailed information required for system programming on all HMIS elements and responses required to be included in HMIS software. It delineates data collection requirements, system logic, and contains the XML and CSV tables and numbers. The manual also includes critical information about data collection stages, federal partner data collection required elements, and metadata data elements.
HMIS Data Standards Manual	HMIS Lead Agencies & HMIS Users	The manual provides a review of all of the Universal Data Elements and Program Descriptor Data Elements. It contains information on data collection requirements, instructions for data collection, and descriptions that the HMIS User will find as a reference.
HMIS Project Descriptor Data Elements Manual	HMIS Lead Agencies	The Project Descriptor Manual is designed to provide specific information about the Project Descriptors required to be set up in the HMIS by the HMIS Lead Agency.

HMIS documents are typically reviewed and updated each year, and changes tend to be effective October 1, in line with the Federal Fiscal Year. HMIS Federal Partner Program Manuals contain additional detailed information on HMIS project setup and data collection for federally-funded programs:

- CoC Program Manual
- ESG Program Manual
- HOPWA Program Manual
- PATH Program Manual
- RHY Program Manual
- VA Program Manual

c. Required Participation in HMIS

Excluding domestic violence service providers (who participate with a comparable database), all programs which receive the following types of funding are required to enter information into HMIS:

- Consolidated Homeless Fund (CHF)
- Continuum of Care (COC)
- State Rental Assistance (HRC)
- Runaway and Homeless Youth (RHY)
- Supportive Services for Veteran Families (SSVF)
- Projects for Assistance in Transition from Homelessness (PATH)
- Cooperative Agreements to Benefit Homeless Individuals (CABHI)

The list above is not exhaustive and other funding sources may require participation in HMIS. All agencies that provide services and housing to the homeless are encouraged to participate in HMIS.

d. Voluntary Participation (Homeless Service Providing Organization)

Although non-funded agencies who agree to participate will meet minimum participation standards, the RICoC strongly encourages any homeless service providers to fully participate with all of their homeless programs, regardless of their funding source.

While each RICoC cannot require non-funded providers to participate in the HMIS, the RICoC works closely with non-funded agencies to articulate the benefits of the HMIS and to strongly encourage their participation. HMIS data provides the best overview available of homelessness in Rhode Island's CoC, and this information is used to redirect services, funding, and resources as needed.

Homeless or housing service providers interested in joining HMIS should contact the HMIS Administrator.

Other organizations who do not provide homeless services or programming may also be interested in joining HMIS for the purposes of care coordination. Please refer to the next section to review those requirements.

e. Read Only Access (Non-Homeless Service Organizations)

Generally, "read only" access to HMIS is not granted to non-homeless service and housing providers. Those in ancillary fields wishing to locate a client, verify information, check assistance status, or review other client level information can make contact with the program serving the client or the Coordinated Entry staff, provided they have an appropriate release. If an organization would like aggregate data on homelessness, they should contact the HMIS Administrator.

Under rare circumstances, the HMIS Steering Committee may make exceptions to this requirement. If an organization would like to request "Read Only Access" and is not a homeless/housing provider, they may submit a letter of interest to the HMIS Steering Committee detailing the following:

1. Agency Information
    a. Contact Information;
    b. Organizational Mission and Work Undertaken;
    c. Documentation that the organization is a government agency or non-profit (with an IRS determination letter, Board of Directors approval, and approved Bylaws);
    d. Documentation the organization has been in operation for over one year;
    e. Agency Privacy and Data Controls; and,
    f. Current Release of Information (if applicable)
2. Reason for Access Request
    a. Intent & Plan for Usage;
    b. Justification for Direct Access to HMIS, as opposed to coordinating with Program Provider/Coordinated Entry Staff;
3. Description of the Staff who will use HMIS; and,
4. Any Other Relevant Information

Voluntary participation in HMIS will be reviewed on an annual basis and organizations may have their access revoked for violations of the requirements set fourth in this manual or at the HMIS Steering Committee's discretion.

This section does not apply to the HMIS Lead agency (and its consultants/contractors), the HMIS Steering Committee Chair, the CoC Collaborative Applicant, the Consolidated Homeless Fund Partnership, funders, and other users designated by the HMIS Steering Committee that have access to HMIS. The HMIS Steering Committee may also approve access to other entities for the purposes of research, analysis, and reporting as described in this document.

f. Points of Contact

HMIS staff is available for Technical Assistance, questions, and trouble-shooting between the hours of 8:30 AM and 4:30 PM Monday to Friday. The HMIS Operations Coordinator and Liaison will try to be available by cell phone (via-text) or e-mail outside of these hours strictly for password resets. An immediate response is not guaranteed based on staff availability and time of day.

HMIS Lead Agency

Rhode Island Coalition for the Homeless
1070 Main Street, Suite 304, Pawtucket, RI 02860
Tel: (401) 721-5685
Fax: (401) 721-5688

Name, Title	Contact	Principal Activities
Caitlin Frumerie, Executive Director	caitlin@rihomeless.org 401-721-5685 x17	Supervision of HMIS team & activities Lead on policy and compliance work
Don Larsen, HMIS Administrator	don@rihomeless.org 401-721-5685 x25	Database and technical system administration Requests for HMIS enhancements or changes Custom report creation Data requests HUD reporting (HIC, PIT, AHAR, CAPER, SPM, LSA, CoC APR etc.) Bed inventory changes Bin/project creation and deactivation Implementation of HUD regulations and data standards Monitoring and ensure privacy and security Agency/User audit reports Adding new users to the system Removing old users from the system Utilizes SAGE for reporting submittals
Bob Maurice, Assistant HMIS Administrator	bob@rihomeless.org 40-721-5685 x 26	Onboarding new users trainings Group user trainings Data quality tracking and technical assistance Installing HMIS security “Certs” Record mergers SAGE/APR report submittals and data quality cleanups Report and system troubleshooting Password Resets
Shalissa Coutoulakis, HMIS Operations Coordinator and Liaison	shalissa@rihomeless.org 401-721-5685 x 27 401-753-2590 (Text-Only for after hour PW Resets)	Liaison for HMIS with CoC, committees, collaborative applicant, coordinated entry system, and other partners Data analysis and visualizations Data and report requests Onboarding of new organizations to HMIS Onboarding new users trainings Group user trainings Data quality tracking and technical assistance Installing HMIS security “Certs” Record mergers Report and system troubleshooting Monthly Newsletters Steering Committee Minutes and Agendas Password Resets SAGE/APR report submittals and data quality cleanups
Emily Howe, Executive Assistant	emily@rihomeless.org 401-721-5685 x 22	Purchase of HMIS Licenses Coordinate with the HMIS Administrator to add new users to System Coordinate with the HMIS Administrator to remove users from the system

CoC Collaborative Applicant
Rhode Island Housing
44 Washington Street, Providence, RI 02903
Tel: (401) 457-1234
Fax: (401) 457-1141

Name, Title	Contact	Principal Activities
Elizabeth Bioteau, Continuum of Care (CoC) Planner	ebioteau@rihousing.com 401-429-1478	CoC Planning and Board Support CoC Program Funding

g. HMIS Steering Committee

The HMIS Steering Committee focuses on strategic policy issues facing the HMIS and submits reports and policy decisions to the RICoC board for review and adoption by the RICoC. The Committee will focus on issues such as data sharing, data quality, data standards, privacy, security, and confidentiality plans, the role of HMIS in coordination of services, and report generation. The Committee generally meets monthly, with HMIS staff coordinating the agenda, sending out meeting notices, and recording/sharing the minutes. Policy updates will be presented to the committee prior to submission to the RICoC board. The RICoC board will present to the RICoC at the next regularly scheduled meeting.

h. Amending the Policies and Procedures

These Policies and Procedures may be amended. It is expected that information shall be added, removed, and altered as necessary. If a change is deemed necessary, it will be vetted by the HMIS Steering Committee and presented to the Board of the Continuum of Care (CoC) for potential adoption by the Rhode Island Continuum of Care (RICoC). Any changes suggested by any party in the RICoC shall be presented by a member of the HMIS Steering Committee or any HMIS staff member to the HMIS Steering Committee. This policy may be amended at any time and the amendments may impact information obtained by the Covered Homeless Organization (CHO) before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

1. On-Boarding of New Agencies to HMIS

a. On-Boarding Procedures

The procedure for onboarding new agencies into HMIS is as follows:

1. Reach out to the HMIS Administrator (and/or HMIS Lead Staff to discuss joining HMIS and its requirements)
2. Identify Agency Administrator.
3. Complete HMIS Partnership Agreement with signatures from the Executive Directors of the Participating Agency, RI Coalition for the Homeless and RI Housing.
4. File Partnership Agreement at RI Coalition for the Homeless.
5. Convene meeting between System Administrator and Agency Administrator to set up project bins in HMIS according to funding source and client population, and to determine the number of End Users/Licenses needed and required permissions.
6. Direct Agency Administrator to HMIS Systems Administrator to purchase required licenses.
7. Ensure Participating Agency has internet connectivity that meets Mediware Systems' requirements.
8. Ensure Participating Agency has suitable computers for HMIS participation.
9. Complete HUD HMIS Security Audit Checklist for Participating Agency.
10. Complete HMIS Security Checklist for each machine that will log on to HMIS.
11. Conduct appropriate trainings for all Participating Agency End Users. Training is considered complete when End Users successfully complete the homework assigned to them and review during the second one-on-one training.
12. Complete HMIS End User Agreement with signatures from Participating Agency Executive Director for each new End User.

* The HMIS System Administrator will provide access to End Users by generating User Names and Passwords upon fulfillment of all above requirements.

b. HMIS Project Set-Up Procedure

When creating new bins (or projects) in ServicePoint, all information relevant to funding and eligibility needs to be collected up front. Bin names need to confirm with HUD's guidance on Project Descriptor Data Elements (i.e. "COC-RRH-FAM" for Continuum of Care funded Rapid Rehousing for Families). Information entered in the ServicePoint Administration Standards tab for each project must align with the project's funding application and the true purpose of the project. To this end, all agencies requesting the creation of new bins must complete the HMIS Project Set-Up Form (obtained from the HMIS Systems Administrator) and send the completed document to their funder if applicable. Upon the funder's verification that the information aligns with original specifications of the project, the System Administrator will create the bin/project in HMIS.

c. Recommended Technical Specifications

For proper access to the HMIS, Participating Agencies should consider the following minimum technology requirements:

A PC with a 2 Gigahertz or higher processor, 40GB hard drive, 512 MB RAM, and Microsoft Windows

7 (or later), Dual-Core processor preferred
The most recent version of Google Chrome, Safari, Internet Explorer, or Firefox. No additional plug-in is required. It is recommended that your browser have a 128 cipher / encryption strength installed. The browser's cache should be set to "Check for new version of the stored pages: Every visit to page."
A broadband Internet connection or LAN connection; Dial-up modem connections are not sufficient.
Up to Date Virus and Malware protection
Mobile devices used for HMIS data entry must use the Mozilla Firefox, Google Chrome, or Apple Safari internet browsers. Apple Safari must be used on the latest version of iOS. (It is important to note that SP-5 is not set-up to be mobile-friendly and may be difficult to use on smart phones or tablets. SP-6 will be mobile-friendly.)
Screen Display of 1024x768 (XGA) or higher; 1280x768 strongly advised

Slow system response times that may arise as a result of slow internet connections cannot be controlled by the HMIS Lead Agency. If there are any Mediware Service Point 'down times' that occur or are expected to occur, the HMIS Systems Administrator will send notice to all participating agencies.

2. Overview of Participating Agency Requirements

a. Collecting Data for HMIS

Agencies participating in the HMIS should collect personal client information ONLY with client consent and when appropriate to provide services and/or for other specific purpose of the organization and/or when required by law. Clients cannot be denied services for choosing not to participate in HMIS.
Purposes for which agencies collect protected personal information (PPI) may include the following:

- to provide or coordinate services to clients;
- to locate other programs that may be able to assist clients;
- for functions related to payment or reimbursement from others for services that are provided;
- to operate the agency, including administrative functions such as legal, audits, personnel, oversight, and management functions;
- to comply with government reporting obligations;
- when required by law; and for research purposes.

b. Eligible HMIS Users

Participating Agencies must have at least one staff member or volunteer who is eligible to become an HMIS user. Users must be *paid staff* or *official volunteers* of an Agency. An official volunteer must complete a volunteer application with the Participating Agency, undergo agency training, and record volunteer hours within their participating agency.

Individuals who are solely contracting with a Participating Agency must be subject to the same

vetting and training as staff and volunteers who become HMIS users. All users must be at least 18 years old and possess basic computer skills. The Participating Agency is responsible for the actions of its users and for their training and supervision, in accordance with the Agency Agreement.

c. Adding New Users to HMIS

Once an organization is approved as a Participating Agency, new users can be requested using this online form: http://sgiz.mobi/s3/HMIS-New-User-License-Request-Form .

d. Participating Agency Administrator Requirements

Agencies must designate one key staff person to serve as Agency Administrator. This person will be responsible for the oversight of all personnel that generate or have access to client data in the HMIS to ensure adherence to the Policies & Procedures described in this document, as well as federal policies and procedures, including HUD publications and updates in the Federal Register. Typically the agency administrator responsibilities include:

- Administering and monitoring agency staff access and use of the HMIS;
- Ensuring compliance with all HMIS policies and procedures through oversight and training of staff, and through creating agency policies that support HMIS policies;
- Preventing staff misuse of the data system by means of training and policy;
- Restricting access to the HMIS to staff who have received proper training, and who have a legitimate need for access (need exists only for those staff who work directly with clients, who supervise staff who work directly with clients, research or have data entry or technical responsibilities);
- Following procedure changes as determined by the HMIS Steering Committee or state and federal regulation;
- Implementing and maintaining data security policies and standards, in compliance with the HMIS Personal Protected Information Policy, the Rhode Island Continuum of Care Authorization to Share Information, and any other applicable policies;
- Administering agency-specified data protection controls;
- Providing assistance in and/or coordinating the recovery of data, when necessary;
- Detecting and responding to violations of federal, HMIS or agency Policies and Procedures;
- Generating Data Quality reports readily available in ServicePoint for Agency projects, and/or reviewing such reports or custom data quality reports generated by HMIS Staff, in order to address data gaps and inconsistencies, at regular intervals each grant year.
- Notify the HMIS Systems Administrator of changes within the Agency Profile, bed counts, changes in funding, when funding ends and when case managers leave their agency.

e. HMIS Partnership Agreement

Agencies must sign and abide by the HMIS Partnership Agreement, a document agreement made between the participating agency and RI Coalition for the Homeless. This agreement includes commitment to enter information on clients served within the agency's participating programs. This document is the legally binding document that refers to all laws and/ or regulations relating to privacy protections and information sharing of client specific information.

f. Security

Agencies must ensure compliance with all requirements set forth in this document including transmission of PPI through unencrypted email.

g. Training

Agencies will ensure that all users meet the mandatory training and onboarding programming requirements. Users who are not trained and/or don't have a current HMIS license in their name, shall not under any circumstances be allowed access to HMIS.

New Users must attend and successfully complete:

1. Part A - One-on-One Training (3 hours – in person)
2. Homework Review (self-paced - remote)
3. Part B - One-on-One Training (1 hours – in person)
4. New User Group Training (1 day - held at RICH)
    a. Part 1 – Rhode Island Homeless System 101 (1.5 hours)
    b. Part 2 - Coordinated Entry (2 hours)
    c. Part 2 – HMIS Training (3 hours)

Once users are trained and licensed, they must attend and successfully complete:

1. ANY two group HMIS trainings each state fiscal year (July 1st–June 30th)
2. One Privacy and Security Group training each state fiscal year (July 1st–June 30th)

Group trainings are offered by RICH on a monthly basis and on demand. Trainings are provided at no cost to users.

At the discretion of the HMIS Lead or RICoC, it may be determined that a user needs to be re-trained and/or that access to HMIS shall be limited until sufficient training can be provided to the user to ensure successful participation in HMIS.

h. HMIS End-User Agreement

Agencies must ensure that each HMIS user signs an "End-User Agreement" which is signed by the End User, a witness, and the Executive Director of the Participating Agency. By signing the agreement, the End User confirms that they understand and will comply with the full scope of HMIS privacy policies, policies regarding access to HMIS, and this document. This includes IT personnel at participating agencies whether or not they are an HMIS user.

i. Data Usage, Sharing and Confidentiality

In accordance with the HUD Data and Technical Standards each agency will read and comply with all policies on usage and release laid out in this manual and associated documents.

j. Data Quality

In accordance with the HUD Data and Technical Standards, End Users will familiarize themselves with the HMIS Data Quality and Monitoring Plan, enter data according to HMIS and HUD Standards,

and cooperate fully with Program Managers and HMIS Staff in correcting aberrations from these standards.

k. Maintenance of On-Site Computer Equipment

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

1. Computer Equipment: The Participating Agency is responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization of HMIS.
2. Internet Connection: The Participating Agency is responsible for maintaining internet connections compatible with daily HMIS usage and troubleshooting problems.
3. Data Storage: The Participating Agency agrees to only download and store data in an encrypted format, using industry standard access controls to secure the data. This may include the use of encrypted archive files such as secured WinZip/PKZip, or the use of operating system security such as data encryption in conjunction with the implementation of system policies to enforce individual user profiles and user authentication. PPI data may not be uploaded/ stored on public sites
4. Data Disposal: The Participating Agency agrees to dispose of documents that contain identifiable client level data in a manner that will protect client confidentiality. Methods may include:
   - Shredding paper records;
   - Deleting any information from media and destroying the media before disposal; and/or
   - Triple formatting hard drive(s) of any machine containing client-identifying information before transfer of property and/or destruction of hard drive(s) of any machine containing client-identifying information before disposal.
5. Data Retention: Protected Personal Information (PPI) that is not in current use seven years after the PPI was created or last changed must be deleted unless a statutory, regulatory, contractual, or other requirement mandates longer retention. Care must be taken to assure that the guidelines associated with Data Disposal are properly followed.

3. Operational Procedures

a. User Accounts

User accounts will be created and deleted by the HMIS Systems Administrator. The HMIS Administrator generates a unique user code for new End Users.

b. Designation of User Access Levels

There are different levels of access to the HMIS. Typically, one person at each agency is designated **Executive Director** (a ServicePoint Access Level), or **Agency Administrator**, and subordinate End Users are designated **Case Manager I**. These permissions are granted based on data entry and management needs. The System Administrator will grant users the access level with the fewest permissions possible that will allow the user to accomplish their job effectively. See the User Role Table in ServicePoint for details.

c. Passwords

ServicePoint generates an initial temporary password for new End Users automatically. The System Administrator provides this password to the new End User. ServicePoint prompts the End User to reset the password immediately, and every 45 days in accordance with federal HMIS password regulations. If a user forgets their password or tries to log-in with 3 failed attempts, the HMIS staff must be contacted in order to request a new password. The temporary password will only work until the user signs in and is asked to reset the password immediately. It is the responsibility of the End Users to select passwords that meet password security guidelines set forth in the HMIS Password Policy and Federal HMIS regulations.

General Requirements:

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- HMIS passwords change every 45 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 60 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

Creation of Passwords:

- Users are to create strong passwords that have the following characteristics:
    - Contain at least three of the five following character classes:
    - Lower case characters
    - Upper case characters

    - Numbers
    - Punctuation
    - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
    - Contain at least eight alphanumeric characters.
    - Try to create passwords that can be easily remembered but hard to guess. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. (NOTE: Do not use either of these examples as passwords!)
- Users are to AVOID creating Weak passwords have the following characteristics:
    - The password contains less than eight characters
    - The password is a word found in a dictionary (English or foreign)
    - The password is a common usage word such as:
        - Names of family, pets, friends, co-workers, fantasy characters, etc.
        - Computer terms and names, commands, sites, companies, hardware, software.
        - The words "Rhode Island Homeless Management Information System (HMIS)", "sanjose", "sanfran" or any derivation.
        - Birthdays and other personal information such as addresses and phone numbers.
        - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
        - Any of the above spelled backwards.
        - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Protection of HMIS Passwords:

- Always use different passwords for HMIS accounts from other passwords
- Do not share HMIS passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential HMIS information.
- Passwords should never be written down or stored online without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Information Security Department.
- Always decline the use of the "Remember Password" feature of applications (e.g., Eudora, Outlook, and Netscape Messenger).
- If an account or password compromise is suspected, report the incident to the Information Security Department.
- Remote access to the HMIS via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Passphrases:

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. All of the rules that apply to passwords apply to passphrases.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper, lowercase letters, and numeric and punctuation characters.

An example of a good passphrase: "The*?#>*@TrafficOnThe101Was*&#!#ThisMorning".

d. Restricting Access

Unauthorized access to the HMIS System must be prevented. User IDs and Passwords are only provided to qualified End Users with legitimate need for access, and inactive user accounts are promptly disabled by the System Administrator. No HMIS license is to be shared and will result in an immediate revocation of HMIS access.

e. Auditing Access

The System Administrator can audit the HMIS System for unauthorized or questionable access of data as a routine security check, or at the request of Agency Administrators or Program Managers.

f. Project Setups and Descriptors

The Project Descriptor Data Elements (PDDE) serves many purposes. PDDEs need to be entered correctly, according to the most recent version of HUD's HMIS Project Descriptor Data Elements Manual, in order to: 1) complete required reports including the APR, LSA , SPMs and HIC; 2) track bed utilization; and 3) calculate rates of HMIS participation. PDDE enables clear identification of projects providing direct service to clients versus those who are the overarching corporate/agency name. The HMIS administrator oversees Project Setups.

g. Using HMIS Data for Research

The HMIS Steering Committee will review and respond to requests for the use of HMIS data for research with the Chair of the Steering Committee having the final decision.

The following procedures will be followed:

- No client protected personal information for any reason may be released to unauthorized entities;
- Only de-identified aggregate data will be released;
- Aggregate data will be available in the form of an aggregate report or as a raw data set;
- Parameters of the aggregate data, that is, where the data comes from and what it includes will be presented with each report;
- Research results will be reported to the HMIS Steering Committee prior to publication, for publication approval by the HMIS Steering Committee;
- Research will be shared with the appropriate agencies after publication; and,
- HMIS Steering Committee will be granted the rights to utilize all findings (results).

Research can be carried out by:

(1) An individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the CHO.

OR

(2) An institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the CHO. A written research agreement must: (1) Establish rules and limitations for the processing and security of PPI in the course of the research. (2) Provide for the return or proper disposal of all PPI at the conclusion of the research. (3) Restrict additional use or disclosure of PPI, except where required by law. (4) Require that the recipient of data formally agree to comply with all terms and conditions of the agreement. A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects' protection institution.

h. Disaster Recovery Plan

Disaster recovery for the Rhode Island Continuum of Care HMIS will be led by the RIHMIS Vendor with support from HMIS Participating Agencies. The HMIS Administrator must be familiar with the disaster recovery plan set in place by the HMIS software vendor.

4. Technical Support

Service requests may be initiated by participating HMIS agency staff to address concerns including, but not limited to, problems logging into HMIS, permissions, visibility, duplicate clients, clarification on data standards, changing bed inventories, adding or removing users, adding or removing bins, problems with data sharing and report writing.

The procedure for a Participating Agency to initiate a technical service request is as follows:

1. End user informs Agency Management Staff (Executive Director or Agency Administrator) of the problem.
2. Agency Management Staff attempts to resolve issue. If unable to resolve, agency staff may contact HMIS staff directly.
3. HMIS staff investigates and addresses the problem or concern if possible.
4. HMIS staff determines resources needed for service and if necessary, contacts vendor for support.
5. Service requests and responses may occur through email, telephone, or in-person appointment as needed.
6. Service requests are handled as promptly as possible, often immediately.

5. Requests for Software Changes and/or Feedback

Users and stakeholders with requests for software changes and/or feedback shall address their concerns to the HMIS Lead's Executive Director and/or the HMIS Steering Committee. Requests for new data elements or questions shall be directed to the HMIS Lead and are not considered Software changes.

6. Data Sharing

a. Statewide Data Sharing

The Rhode Island CoC employs statewide data sharing as a means to coordinate care, implement Coordinated Entry, reduce data collection and entry burden, and facilitate other coordination between Participating Agencies.

b. Client Release of Information

Statewide Data Sharing is a process guided by the client through the Release of Information (ROI). It is therefore imperative that the client understand the ROI, and that the Participating Agency address any questions the client may have, while respecting the client's right to decline to share data.

Prior to entering information into HMIS, the Participating Agency will obtain the informed (written or verbal) consent of the Client, with written consent preferred, using the HMIS Release of Information. If a client does not consent pursuant to the HMIS Release of Information (ROI) form, information may not be entered into HMIS.

It is the responsibility of the agency entering information about a client to determine whether consent has been obtained; to make appropriate entries to either designate the information as appropriate for sharing or prohibit information sharing; and to implement any restrictions on information sharing.

At a minimum, the Participating Agency must meet the following standards:

- The Participating Agency will use the HMIS Release of Information form (ROI), for all clients where written or verbal consent is required.
    - If the Participating Agency does not share data with other Agencies, the ROI form is not required. However, the Participating Agency will provide Rhode Island's HMIS Data Privacy Notice for review by all clients and provide clients with copies as requested.
    - If questions arise (for example questions on which programs within the Participating Agency share data with other agencies), the Participating Agency will contact the Lead Agency.

- The Participating Agency will note any limitations or restrictions on information sharing on a client's ROI with appropriate data entries into HMIS. If questions arise (for example, questions on how to implement restrictions on information sharing), the Participating Agency will contact the HMIS Lead.
- The Participating Agency will be responsible for ensuring that consent is understood and given by a person competent to provide consent. For example, in the case of a minor, the Participating Agency will comply with applicable laws regarding minor consent or obtain the consent of a parent or guardian.

- If a client withdraws or revokes consent for release of information, the Participating Agency is responsible for immediately contacting the HMIS Lead Agency to ensure that client's information will not be shared with other Agencies from that date forward.
- The Participating Agency that received the client's initial ROI form will scan and upload the signed copy of the form to the HMIS. Participating Agencies may be required to keep the original copy for a period of seven years, as dictated by Participating Agency policy or funder requirements. ROI forms will be available for inspection and copying by the Lead Agency at any time.
- If an ROI has been properly recorded in the client's HMIS record by another Participating Agency, the Participating Agency need not present the client with another ROI form. However, Covered Entities must always present a ROI form, as detailed in the section below. Other Participating Agencies may elect to do so at their discretion.

Additional Responsibilities of Covered Entities (HIPAA)

Participating Agencies that are also Covered Entities under the Health Insurance Portability and Accountability Act (HIPAA) and any program subject to 42 CFR Part 2 must obtain a signed HMIS Release of Information form before authorizing the Lead Agency to use or disclose information entered into the HMIS.

The information may be used by the Lead Agency as permitted by law and the HMIS Data Privacy Notice. It is the responsibility of the Participating Agency entering information about a client to ensure compliance with HIPAA including ensuring that all appropriate HIPAA Notices have been provided to clients, to determine whether consent has been obtained; making appropriate entries to either designate the information as appropriate for use or disclosure by the Lead Agency or to prohibit such use or disclosure; and implementing any restrictions on the use of the information.

The requirement to scan and upload signed Consent forms is effective as of the date these policies were first adopted. Client records created prior to that date that recorded Consent according to the guidance from that time are considered to have Consent properly recorded. Covered Entities may utilize their own forms but shall supplement these forms with the information conveyed in this document. Covered Entities must present a separate ROI form to each adult that is seeking services, regardless of whether a ROI form has been presented to them in the past.

c. No Conditioning of Services based on Release of Information

Participating Agencies will not condition any services upon or decline to provide any services to a client based upon a client's refusal to sign a form for the sharing of information in HMIS, unless a program funder or internal management practices require the entry of identified information into the HMIS to deliver services. Further, Participating Agencies may not limit client service or refuse to provide service in a way that discriminates against clients based on information the Participating Agency obtained from the HMIS. Participating Agencies may not penalize a client based on historical data contained in the HMIS.

d. Sharing of Attachments

Uploaded client documents and attachments shall be shared Statewide, provided the client has signed a consent to have that information shared as of the date indicated on the signed release. The default setting in HMIS as of that date is to share all attachments Statewide. If the client HAS NOT signed a "Attachment Consent Form", you must note that in HMIS, and contact the HMIS Administrator at RICH in order to restrict access to the document. Sharing of attachments will allow for better care coordination, support coordinated entry, reduce duplication of collection of vital documents, and ensure safe digital keeping of important client records.

e. Reporting Access

Generally, individual participating agencies shall only have access to pull reports on their specific programs, activities, and projects. Organizations may enter into agreements with one another to allow other organizations access to agency/project reports and aggregate data.

HMIS Participating agencies may also submit a request to the HMIS Steering Committee to have the HMIS Lead pull a report that includes other participating agencies (e.g. organization wants a report on all rapid rehousing outcomes, not just their own programs). Any requests submitted to the HMIS Steering Committee will be shared with the organizations whose data is requested and their input sought, before a final decision is made.

Only the HMIS Lead agency (and its consultants/contractors), the HMIS Steering Committee Chair, the CoC Collaborative Applicant, the Consolidated Homeless Fund Partnership, funders, and other HMIS Steering Committee designated users can have access to aggregate reports and data. The HMIS Steering Committee may also allow access to other entities for the purposes of research, analysis, and reporting.

Note that this section applies only to aggregate and project level reporting and is not be confused with data sharing on a client level basis, which is covered in the following sections.

7. Privacy

a. Introduction

The HMIS Lead Agency, Participating Agencies, and End Users are jointly responsible for complying with HMIS privacy policies and procedures. When a privacy standard conflicts with other federal, state and local laws to which the Participating Agency must adhere, the Participating Agency must contact the Lead Agency to collaboratively update the applicable policies for the Participating Agency to accurately reflect the additional protections.

We intend our Privacy Plan to support our mission of providing an effective and usable case management tool. We recognize that clients served by individual agencies are not exclusively that "agency's client" but instead are truly a client of the RI Continuum of Care. Thus, we have adopted a Privacy Plan which supports an open system of client-level data sharing amongst agencies.

HMIS Privacy and Security standards are set forth by HUD and outlined in HUD's standards for Homeless Management Information Systems (69 Federal Register 45888) and on December 9, 2011 HUD released *HMIS Requirements Proposed Rule* (*Federal Register Vol. 76, No. 237 Friday, December 9, 2011 Proposed Rules)*.

b. Baseline Privacy

The core tenant of our Privacy Plan is the Baseline Privacy Statement. The Baseline Privacy Statement describes how client information may be used and disclosed and how clients can get access to their information.

Each agency must either adopt the Baseline Privacy Statement or develop a Privacy Statement which meets and exceeds all minimum requirements set forth in the Baseline Privacy Statement (this is described in the Agency Responsibilities section of this Privacy Plan). This ensures that all agencies who participate in the HMIS are governed by the same minimum standards of client privacy protection.

Summary Required Elements & Documents	
Baseline Privacy Statement: This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency collects, utilizes, and discloses information.	Agencies must adopt a privacy statement which meets all minimum standards. It is must be posted on your Agency's local website (if available).
Consumer Notice Posting: This posting explains the reason for asking for personal information and notifies the client of the Privacy Notice.	Agencies must adopt and utilize a Consumer Notice Posting.
Consumers Informed Consent, Sharing & Release of Information Authorization: This form must be signed by all adult clients and unaccompanied youth. This gives the client the opportunity to refuse the sharing of their information to other agencies within HMIS.	Client Signatures are required prior to inputting their information in HMIS.

c. End User Privacy Responsibilities

A client's privacy is upheld only to the extent that the users and direct service providers protect and maintain client's privacy. The role and responsibilities of the user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client or their data. (This could potentially be any person at the agency: staff member, volunteer, contractor, etc.)

Users have the responsibility to:

- Understand their agency's Privacy Statement
- Be able to explain their agency's Privacy Statement to clients
- Follow their agency's Privacy Statement
- Know where to refer the client if they cannot answer the client's questions
- Must complete Consumers Informed Consent, Sharing & Release of Information Authorization
- with client prior collecting HMIS data.
- Present their agency's Privacy Statement to the client before collecting any information

- Uphold the client's privacy in the HMIS

d. Participating Agency Responsibilities

This Privacy Plan and the Baseline Privacy Statement provide guidance on the minimum standards by which agencies must operate if they wish to participate in the HMIS. Meeting the minimum standards in this Privacy Plan and the Baseline Privacy Statement are required for participation in the HMIS. Any agency may exceed the minimum standards described and are encouraged to do so. Agencies must have an adopted Privacy Statement which meets the minimum standards before data entry into the HMIS can occur.

Agencies have the responsibility to:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in this Privacy Plan and Baseline Privacy Statement (examples: Substance Abuse Providers covered by State Law, 24 CFR Part 2, HIPPA Covered Agencies, Legal Service Providers).
- Review the 2004 HUD HMIS Privacy Standards (69 Federal Register 45888)
- Adopt and uphold a Privacy Statement which meets or exceeds all minimum standards in the Baseline Privacy Statement as well as all industry privacy standards. The adoption process is to be directed by the individual agency. Modifications to the Baseline Privacy Statement must be presented to the HMIS Steering Committee and approved by the RICoC.
- Ensure that all clients are aware of the adopted Privacy Statement and have access to it. If the agency has a website, the agency must publish the Privacy Statement on their website.
- Make reasonable accommodations for persons with disabilities, language barriers, or education barriers.
- Ensure that anyone working with clients covered by the Privacy Statement can meet the User Responsibilities.
- Designate at least one Security Officer that has been trained to uphold technologically the agencies adopted Privacy Statement.

Each HMIS Participating Agency must have a Privacy Statement that describes how and when the Participating Agency may use and disclose clients' Protected Personal Information (PPI). PPI includes but is not limited to name, Social Security Number (SSN), date of birth, project entry and/or exit date, and unique personal identification number (HMIS Unique Identifier).

Participating Agencies may be required to collect some PPI by law, or by organizations that give the agency money to operate their projects. PPI is also collected by Participating Agencies to monitor project operations, to understand better the needs of people experiencing homelessness, and to improve services for people experiencing homelessness. Participating Agencies are permitted to collect PPI only with a client's written consent.

e. Use and Disclosure of Information

Participating Agencies may use and disclose client PPI to:

- Undertake tasks as outlined in the Release of Information;
- Verify eligibility for services;
- Provide clients with and/or refer clients to services that meet their needs;

- Manage and evaluate the performance of projects;
- Report about project operations and outcomes to funders and/or apply for additional funding to support agency projects;
- Collaborate with other local agencies to improve service coordination, reduce gaps in services, and develop community-wide strategic plans to address basic human needs; and,
- Participate in research projects to understand better the needs of people served.
- Participating Agencies may also be required to disclose PPI for the following reasons:
    - When the law requires it;
    - When necessary to prevent or respond to a serious and imminent threat to health or safety; or,
    - When a judge, law enforcement or administrative agency orders it.

Participating Agencies are obligated to limit disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures of PPI not described above may only be made with a client's written consent. Clients have the right to revoke consent at any time by submitting a request in writing.

f. Clients Access to Records

Clients also have the right to request from HMIS:

- A copy of all PPI collected;
- An amendment to any PPI used to make decisions about your care and services (this request may be denied at the discretion of the agency, but the client's request should be noted in the project records);
- An account of all disclosures of client PPI;
- Restrictions on the type of information disclosed to outside partners; and,
- A current copy of the Participating Agency's privacy statement.

Participating Agencies may reserve the right to refuse a client's request for inspection or copying of PPI in the following circumstances:

- Information compiled in reasonable anticipation of litigation or comparable proceedings;
- The record includes information about another individual (other than a health care or homeless provider);
- The information was obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) and a disclosure would reveal the source of the information; or,
- The Participating Agency believes that disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If a client's request is denied, the client should receive a written explanation of the reason of the denial. The client has the right to appeal the denial by following the established Participating Agency grievance procedure. Regardless of the outcome of the appeal, the client shall have the right to add to his/her program records a concise statement of disagreement. The Participating Agency shall disclose the statement of disagreement whenever it discloses the disputed PPI.

g. Privacy Training

All individuals with access to PPI are required to complete formal training in privacy

requirements at least annually.

h. Participating Agency Privacy Statements

Participating Agency Statements should, at a minimum, reflect the baseline requirements listed in this document and the HMIS Data and Technical Standards Final Notice, published by HUD in July 2004, and revised in March 2010. In any instance where this Privacy Statement is not consistent with the HUD Standards, the HUD Standards take precedence except where an agency is acting as a HIPAA entity Participating Agency Privacy Statements may be amended at any time. Amendments may affect information obtained by the agency before the date of the change. An amendment to the Privacy Statement regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. A record of all amendments to this Privacy Statement must be made available to clients upon request.

8. Security

a. Security Plan Overview

HMIS security standards are established to ensure the confidentiality, integrity, and availability of all HMIS information. The security standards are designed to protect against any reasonably anticipated threats or hazards to security and must be enforced by system administrators, agency administrators, as well as end users. This section is written to comply with section 4.3 of the 2004 Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice (69 Federal Register 45888) as well as local legislation pertaining to maintaining an individual's personal information. The last time HUD has released proposed regulations pertaining to HMIS Security was in December of 2013. These regulations are not yet in force and sufficient guidance has not been given to enact the policies.

The HMIS System and all agencies must apply the security standards addressed in this Security Plan to all the systems where personal protected information is stored or accessed. Additionally, all security standards must be applied to all networked devises. This includes, but is not limited to, networks, desktops, laptops, mobile devises, mainframes, and servers. Agencies IT people; whether or not they enter information into HMIS must sign a User Agreement.

All agencies, including the HMIS Lead, will be monitored by the HMIS Administrators annually to ensure compliance with the Security Plan. Agencies that do not adhere to the security plan will be given a reasonable amount of time to address any concerns. Egregious violations of the security plan may result in immediate termination of an agency or user's access to the HMIS as determined by the HMIS Lead.

b. Security Officers

The HMIS Lead Agency and all HMIS Participating Agencies must designate Security Officers to oversee HMIS privacy and security. The security officer is the single point-of-contact who is responsible for annually certifying that Agencies adhere to the Security Plan testing the CoC's security practices for compliance.

Systemwide Security Officer

Position held by the Assistant HMIS Administrator and is responsible for:

- Assessing security measures in place prior to establishing access to HMIS for a new Agency,
- Reviewing and maintaining file of Participating Agency annual compliance certification checklists,
- Conducting annual security audit of all Participating Agencies.

Participating Agency Security Officer

Position fulfilled within a Participating Agency, may be the agency administrator or another employee, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance.

This person:

- Conducts a security audit for any workstation that will be used for HMIS purposes,

- Conducts a security audit no less than annually for all agency HMIS workstations, AND
- Continually ensures each workstation within the Participating Agency used for HMIS data collection or entry is adequately protected by a firewall and antivirus and malware software (per Technical Safeguards – workstation computer policy),
- Completes the semi-annual Compliance Certification Checklist, and forwards the Checklist to the Lead Security Officer.

Upon request, the HMIS Lead Agency may be available to provide Security support to Participating Agencies who do not have the staff capacity or resources to fulfill the duties assigned to the Participating Agency Security Officer.

c. Physical Safeguards

In order to protect client privacy, it is important that the following physical safeguards be put in place. For the purpose of this section, authorized persons will be considered only those individuals who have completed Privacy and Security training within the past 12 months.

- Computer Location – A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The workstation must not be accessible to clients, the public or other unauthorized Participating Agency staff members or volunteers. A password protected automatic screen saver will be enabled on any computer used for HMIS data entry.
- Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.
- PC Access (visual) — Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized Participating Agency staff members or volunteers and utilize visibility filters to protect client privacy.
- Mobile Device – A mobile device used to access and enter information into the HMIS system must use a password or other user authentication on the lock screen to prevent an unauthorized user from accessing it and it should be set to lock automatically after a set period of device inactivity. A remote wipe and/or remote disable option should also be downloaded onto the device.

d. Technical Safeguards

Workstation Security

To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations. The HMIS Lead Agency will be required to have and install a PKI certificate on all approved workstations, in compliance with Public Access baseline requirement in the HUD Data Standards (4.3.1 System Security). End-Users will be required to have this certificate installed on each individual account for each HMIS user of their workstation by the HMIS Lead Agency and will notify the Lead Agency should this certificate need to be re-installed or the computer decommissioned.

Participating Agency Security Officer will confirm that any workstation accessing HMIS shall have

antivirus, antimalware software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly).

Participating Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall either on the workstation itself if it accesses the internet through a modem or on the central server if the workstation(s) accesses the internet through the server.

Establishing HMIS User IDs and Access Levels

The HMIS Administrator, in conjunction with the Participating Agency Executive Director, will ensure that any prospective End User reads, understands, and signs the HMIS End User Agreement. The HMIS Administrator will maintain a file of all signed HMIS End User Agreements. The Participating Agency is responsible for ensuring that all agency End Users have completed mandatory trainings, including HMIS Privacy and Security training and End User Responsibilities and Workflow training, prior to being provided with a User ID to access HMIS.

The HMIS Administrator will always attempt to assign the most restrictive access that allows an End User to perform efficiently and effectively their duties. The HMIS Administrator will also create new User IDs and notify the User ID owner of the temporary password verbally. When the Participating Agency determines that it is necessary to change a user's access level, the HMIS Administrator will update the user's access level as needed.

User Authentication

User IDs are individual and passwords are confidential. No individual should ever use or allow use of a User ID that is not assigned to that individual, and user- specified passwords should never be shared or communicated in any format.

End users will be prompted by the software to change their password every 45 days.

End Users must immediately notify the HMIS Administrator if they have reason to believe that someone else has gained access to their password.

Three consecutive unsuccessful attempts to login will disable the User ID until the password is reset. For Agency End Users, passwords should be reset by one of the HMIS contacts.

Rescinding User Access

The Participating Agency must notify the HMIS Administrator within 24-hours if an End User no longer requires access to perform his or her assigned duties due to a change of job duties or termination of employment. The HMIS Administrator reserves the right to terminate End User licenses that are inactive for 60 days or more. The HMIS Administrator will attempt to contact the Participating Agency for the End User in question prior to termination of the user's license.

In the event of suspected or demonstrated noncompliance by an End User with the HMIS End User Agreement or any other HMIS plans, forms, standards or governance documents, the Participating Agency Security Officer shall notify the HMIS Administrator to deactivate the User ID for the End User in question until an internal agency investigation has been completed. The HMIS Lead Agency should be notified of any substantiated incidents that may have resulted in a breach of HMIS system security and/or client confidentiality, whether or not a breach is definitively known to have occurred.

Any agency personnel who are found to have misappropriated client data (identity theft, releasing personal client data to any unauthorized party), shall have HMIS privileges revoked. The Continuum of Care is empowered to revoke permanently a Participating Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Rhode Island HMIS CoC Policies and Procedures, or the HMIS Privacy Statement that resulted in a release of PPI.

e. Workstation Security

RI HMIS Users will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Specific measures include:

- Restricting physical access to workstations to only authorized personnel;
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access;
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected;
- Complying with all applicable password policies and procedures;
- Ensuring workstations are used for authorized business purposes only;
- Never installing unauthorized software on workstations;
- Storing all sensitive information, including protected health information (PHI) on network servers;
- Keeping food and drink away from workstations in order to avoid accidental spills;
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets;
- Ensuring workstations are updated regularly or left on but logged off in order to facilitate IT after-hours updates. Remember to exit running applications and close open documents;
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup); and,
- If wireless network access is used, ensure access is secure by following the Wireless Access policy

Workstations include any areas or devices used to access HMIS or undertake work on HMIS (including spaces at home, office, and remote locations). Specific devices include but are not limited to laptops, tablets, phones, mobile devices, desktops, and computer based medical equipment.

f. Disposing Electronic, Hardcopies, Etc.

Computer: All technology equipment (including computers, printers, copiers and fax machines) used to access HMIS and which will no longer be used to access HMIS will have their hard drives reformatted multiple times (DoD specifications). If the device is now non-functional, it must have the hard drive pulled, destroyed, and disposed of in a secure fashion.

Hardcopies: For paper records, shredding, burning, pulping, or pulverizing the records so that PPI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

Mobile Devices: Use software tools that will thoroughly delete/wipe all information on the device and return it to the original factory state before discarding or reusing the device.

g. Other Technical Safeguards

The Lead Security Officer shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.

The Participating Agency Security Officer shall develop and implement procedures for managing new, retired, and compromised local system account credentials. The Participating Agency Security Officer shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks.

Unencrypted PPI may not be stored or transmitted in any fashion—including sending file attachments by email or downloading reports including PPI to a flash drive, to the End User's desktop or to an agency shared drive. All downloaded files containing PPI must be deleted from the workstation temporary files and the "Recycling Bin" emptied before the End User leaves the workstation.

h. Reporting Security Incidents

These standards are intended to prevent, to the greatest degree possible, any security incidents. However, should a security incident occur, the following procedures should be followed in reporting:

- Any HMIS End User who becomes aware of or suspects that HMIS system security and/or client privacy has been compromised must immediately report the concern to their Participating Agency Security Officer.
- In the event of a suspected security or privacy concern the Participating Agency Security Officer should complete an internal investigation. If the suspected security or privacy concern resulted from an End User's suspected or demonstrated noncompliance with the HMIS End User Agreement, the Participating Agency Security Officer should have the HMIS Administrator deactivate the End User's User ID until the internal investigation has been completed.
- Following the internal investigation, the Participating Agency Security Officer shall notify the Lead Security Officer of any substantiated incidents that may have compromised HMIS system security and/or client privacy whether or not a release of client PPI is definitively known to have occurred. If the security or privacy concern resulted from demonstrated noncompliance by an End User with the HMIS End User Agreement, the Lead Security Officer reserves the right to deactivate permanently the User ID for the End User in question.
- Within one business day after the Lead Security Officer receives notice of the security or privacy

concern, the Lead Security Officer and Participating Agency Security Officer will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent such future concerns. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed thirty (30) days.

- If the Participating Agency is not able to meet the terms of the action plan within the time allotted, the HMIS Administrator, in consultation with the Rhode Island Continuum of Care Advisory Board, may elect to terminate the Participating Agency's access to HMIS. The Participating Agency may appeal to the CoC Advisory Board for reinstatement to HMIS following completion of the requirements of the action plan.
- In the event of a substantiated release of PPI in noncompliance with the provisions of these Security Standards, the Rhode Island HMIS Policies and Procedures, or the Participating Agency Privacy Statement, the Participating Agency Security Officer will make a reasonable attempt to notify all impacted individual(s). The Lead Security Officer must approve of the method of notification and the Participating Agency Security Officer must provide the Lead Security Officer with evidence of the Agency's notification attempt(s). If the Lead Security Officer is not satisfied with the Agency's efforts to notify impacted individuals, the Lead Security Officer will attempt to notify impacted individuals at the Agency's expense.
- The HMIS Lead Agency will notify the appropriate body of the Continuum of Care of any substantiated release of PPI in noncompliance with the provisions of these Security Standards, the HMIS Policies and Procedures, or the Participating Agency Privacy Statement.
- The HMIS Lead Agency will maintain a record of all substantiated releases of PPI in noncompliance with the provisions of these Security Standards, the Rhode Island HMIS Policies and Procedures, or the Participating Agency Privacy Statement for 7 years.
- The Continuum of Care reserves the right to revoke permanently a Participating Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Rhode Island HMIS Policies and Procedures, or the Participating Agency Privacy Statement that resulted in a release of PPI.

i. New HMIS Participating Agency Site Security Assessment

Prior to establishing access to HMIS for a new Participating Agency, the Lead Security Officer will assess the security measures in place at the Participating Agency to protect client data (see Technical Safeguards Workstation Security). The Lead Security Officer or other HMIS Administrator will meet with the Participating Agency Executive Director (or executive-level designee) and Participating Agency Security Officer to review the Participating Agency's information security protocols prior to countersigning the HMIS Memorandum of Understanding. This security review shall in no way reduce the Participating Agency's responsibility for information security, which is the full and complete responsibility of the Participating Agency, its Executive Director, and its HMIS Agency Security Officer.

j. Annual Participating Agency Self-Audits

- The Participating Agency Security Officer will use the Compliance Certification Checklist to conduct annually security audits of all Participating Agency HMIS End User workstations.
- The Participating Agency Security Officer will audit for inappropriate remote access by End-Users by associating User login date/times with employee time sheets. End Users must certify that they will not remotely access HMIS from a workstation (i.e.: personal computer) that is not subject to the Participating Agency Security Officer's regular audits.
- If areas are identified that require action due to noncompliance with these standards or any element of the Rhode Island HMIS Policies and Procedures, the Participating Agency Security Officer will note

these on the Checklist, and the Participating Agency Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within 15 days.

- Any Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved. The findings, action items, and resolution summary must be reviewed and signed by the Agency's Executive Director or other empowered officer prior to being forwarded to the Lead Security Officer.
- The Participating Agency Security Officer must turn in a copy of the Checklist to the Lead Security Officer on a semiannual basis.

k. Annual Security Audits

- The Lead Security Officer will use the Compliance Certification Checklist to conduct security audits.
- The Lead Security Officer must randomly audit at least 10% of the workstations used for HMIS data entry. In the event that an agency has more than 1 project site, at least 1 workstation per project site must be audited.
- If areas are identified that require action due to noncompliance with these standards or any element of the Rhode Island HMIS Policies and Procedures, the Lead Security Officer will note these on the Checklist, and the Participating Agency Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within 15 days.
- Any Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the findings, action items, and resolution summary has been reviewed and signed by the Agency's Executive Director or other empowered officer and forwarded to the HMIS Lead Security Officer.

9. Client Complaints, Grievances, and Questions

If a client believes that their rights have been violated related to their personal or private data held in the HMIS, a written complaint may be filed. The complaint may be filed with the Participating Agency serving the client and forwarded to the HMIS Lead Agency if resolution is not found. If the client believes that their shelter or services may be threatened due to the complaint, a complaint may be made directly to the HMIS Lead Agency. The Lead Agency will report all grievances to the HMIS Steering Committee (which reports up to the CoC Board). The HMIS Steering Committee will act as a final arbiter of any complaints not resolved by the Participating Agency or the Lead Agency.

The Participating Agency and HMIS Lead Agency are prohibited from retaliating against clients for filing a complaint. Identifying information will be kept confidential, unless the client gives express permission for such information to be shared between the Participating Agency and the HMIS Lead Agency.

10. Violation of HMIS Policies

HMIS users and Participating Agencies must abide by all HMIS policies and procedures found in the HMIS Policies and/or Procedures manuals, the User Agreement, and the Agency Agreement.

Participating Agency or user access may be suspended or revoked for suspected or actual violation of these policies, particularly the security protocols. Serious or repeated violation by users of the system may result in the suspension or revocation of a participating agency's access.

Any user or other fees paid by the Participating Agency will not be returned if a user's or Participating Agency's access to the HMIS is revoked.

The procedure to be followed is:

1. All suspected violations of any security protocols will be investigated by the Participating Agency and the HMIS Lead.
2. Any user found to be in violation of security protocols will be sanctioned by his/her agency. Sanctions may include but are not limited to a formal letter of reprimand, suspension of HMIS privileges, and revocation of HMIS privileges.
3. Access may be restricted prior to completion of formal investigation if deemed necessary by the HMIS Lead. If access is restricted, the HMIS Lead will notify a chair of the HMIS Steering Committee of the restriction and will consult with him/her about next steps.
4. Any Participating Agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.
5. All sanctions can be appealed to the HMIS Steering Committee.

Notifying the HMIS Lead Agency of a Violation

It is the responsibility of each Designated Agency HMIS Contact and user to notify the HMIS Lead Agency within 24 hours of when they suspect that a User or Participating Agency has violated any HMIS operational agreement, policy, or procedure. A complaint about a potential violation must include the User and Participating Agency name and a description of the violation, including the date or timeframe of the suspected violation. Complaints should be sent in writing to the HMIS Lead Agency. The name of the person making the complaint will not be released from the HMIS Lead Agency if the individual wishes to remain anonymous.

Violations of Local, State or Federal Law

Any Participating Agency or user violation of local, state or federal law will immediately be subject to the consequences listed under the Third Violation above.

11. Glossary and Definitions

AHAR – Stands for the Annual Homeless Assessment Report; HUD (the United States Department of Housing and Urban Development) uses the AHAR to report to U.S. Congress that provides nationwide estimates of homelessness. Soon to be replaced by the LSA (definition below).

Bin – A basic project organizational unit in ServicePoint. One agency may have several bins which are associated with different project locations, funding, or types of services provided.

CAPER – Stands for the Consolidated Annual Performance and Evaluation Report; Generated to report on accomplishments and progress towards consolidated plan goals.

CoC APR – the HUD Continuuon of Care (CoC) Annual Performance Report (APR) is used for any recipients with HUD funding received through CoC homeless assistance grants are required to submit an APR electronically to HUD every operating year.

CoC Board - The RICoC consists of a Board of Directors, a membership group, and 6 standing committees (System Performance & Planning, Recipient Approval & Evaluation, Veterans, Families & Youth, Chronically Homeless/High Needs Individuals, and HMIS).

Continuum of Care (CoC) - A Continuum of Care (CoC) is a regional or local planning body that coordinates housing and services funding for homeless families and individuals.

Covered Homeless Organization (CHO) - An organization that records, uses, or processes personal protected information on homeless clients for HMIS

HEARTH Act- On May 20, 2009, President Obama signed the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009. The HEARTH Act amends and reauthorizes the McKinney-Vento Homeless Assistance Act with substantial changes; including a consolidation of HUD's competitive grant programs, the creation of a Rural Housing Stability Assistance Program, a change in HUD's definition of homelessness and chronic homelessness, a simplified match requirement, an increase in prevention resources and emphasis on performance.

HIC – Stands for Housing Inventory Count; HUD requires CoC's to conduct an annual count of homeless persons and the HIC is a point-in-time inventory pf provider programs within a CoC that provide beds and units dedicated to serve persons who are homeless, categorized by five program types: Emergency Shelter (ES), Transitional Housing (TH), Rapid Re-Housing (RRH), Safe Haven (SH), and Permanent Supportive Housing (PSH).

HMIS – Stands for Homeless Management Information System, which is a local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals, families, and persons at risk of homelessness.

HMIS Lead Agency – The HMIS Lead Agency is the Rhode Island Coalition for the Homeless. This entity is designated by the Continuum of Care to operate the Continuum's HMIS on its behalf.

HMIS Steering Committee – Comprised of HMIS stakeholders, this committee focuses on strategic and policy issues facing the HMIS, such as data sharing, data quality standards, privacy, security, and report generation.

HUD - The United States Department of Housing and Urban Development is a Cabinet department in the Executive branch of the United States federal government that funds permanent housing and emergency shelter services for homeless and formerly homeless individuals and families. An HMIS system is required by HUD for all CoCs receiving HUD funding.

Longitudinal Systems Analysis (LSA) report – used to replace the AHAR, is produced from a CoC's Homelessness Management Information System (HMIS) and submitted annually to HUD via the HDX 2.0, provides HUD and Continuums of Care (CoCs) with critical information about how people experiencing homelessness use their system of care.

Participating Agency – An Agency within the RICoC that creates, edits or views HMIS data.

PIT – Stands for Point-in-Time count; HUD requires a count of sheltered and unsheltered homeless persons on a single night in January – this count includes persons who are sheltered in an Emergency Shelter (ES) or Transitional Housing (TH) as well as those unsheltered on the street or in a place not meant for human habitation. PITs are collected annually including the last Wednesday of each quarter.

Project – A distinct unit of an organization that provides services and/or lodging and is identified by the CoC as part of its service system; A continuum project can be classified as one that provides lodging (lodging project) or one that does not provide lodging (services project). Projects are equated with bins in HMIS

Protected Personal Information (PPI) - Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

RICoC - Rhode Island has a single Continuum of Care (RICoC) which guides the state's homelessness programs and policies, and administers federal and state homeless funds. The continuum includes a broad range of state agencies, community partners, and individuals all working together to build a statewide system to prevent and end homelessness.

ServicePoint – A web-based software interface for the HMIS database, created by Mediware. Rhode Island contracts with Mediware to use ServicePoint for HMIS.

12. Attachments

The attachments listed below can be found on the Rhode Island Coalition for the Homeless' website, which can be found at the following link: https://www.rihomeless.org/hmis-information-forms-and-guides.

The website includes the most up-to-date and recent version of all documents related to HMIS such as (but not limited to):

1. The HMIS Release of Information (ROI)
2. The Personal Protected Information Statement
3. The HMIS Data Collection Statement
4. The HMIS Fact Sheet
5. The HMIS User Agreement
6. The Checklist for the HMIS Certificate Installation
7. The Desktop and Mobile Devices Agreement
8. The RICoC VI-SPDAT Policy
9. HUD HMIS Data Standards Manual and Dictionary

13. Acknowledgements & Revision History

This HMIS Policy and Procedures Handbook was collaboratively written and informed by versions of other HMIS Policies and Procedure Documents from communities.

March 2005

January 2007

August 2013

March 2017

September 2018