VA-514 Fredericksburg Regional CoC
FY21 VHSP Application

Attachment 7: CoC/LPG HMIS Policies and Procedures

Note: The Fredericksburg Regional CoC contracts with Homeward, lead agency of the Greater Richmond CoC, for HMIS service, known as the Homeward Community Information System (HCIS). These policies and procedures are in the process of being updated and approved by all CoCs with the HCIS implementation. The Fredericksburg Regional CoC Board approved the revisions during their meeting on February 6, 2020.

Homeward Community Information System

Policies and Procedures

Revised 11/8/19

Table of Contents

Introduction

The Homeward Community Information System (HCIS) is a HIPAA-compliant online database used to record and retrieve client-level and systems-level data. Homeward of Richmond, Virginia is a 501(c)(3) non-profit organization that maintains the HCIS using ServicePoint, a software application provided under contract with WellSky (formerly known as Bowman Systems/Mediware).

Agencies that participate in the HCIS have access to a common set of tools and agree to uphold standards of privacy and confidentiality as a condition of continued use. Staff of Partner Agencies may enter data on clients and services, case plans and client goals, follow-up actions, and referrals to other agencies. Homeward provides technology recommendations, business integration, training and technical assistance to agencies and users participating in the system.

In using ServicePoint, the HCIS is a Homeless Management Information System (HMIS) of the kind required by the U.S. Department of Housing and Urban Development (HUD) and Virginia Department of Housing and Community Development (DHCD). It may also satisfy the requirements of other funding sources.

This document provides the policies, procedures, guidelines, and standards that govern the HCIS, as well as roles and responsibilities for authorized representatives and Partner Agency staff.

Definitions

Terms

In this Policies and Procedures Manual ("Policies and Procedures"), "Partner Agencies" are all Agencies participating in the HCIS; "User" is a person accessing the HCIS; and "Client" is a consumer of services at a Partner Agency.

Personally Identifying Information

Data is considered "personally identifying" if it can be used alone or in combination with another data source to identify an individual. This includes, but is not limited to: name, date of birth, social security number, telephone number or numbers, any part of an address, photographs, email address, driver's license number, license plate number, the number of any other professional certification or license, and any other characteristic that could uniquely identify the individual.

Governing Principles

Described below are the overall governing principles upon which all other decisions pertaining to the HCIS are based.

Data Integrity

Data is the most valuable asset of the HCIS. It is the responsibility of each and every user to protect data from unauthorized release, disclosure, modification, or destruction.

Partner Agencies are also required to input at least the minimum data elements as prescribed by the Department of Housing and Urban Development (HUD) for Homeless Management Information Systems (HMISs). Additionally, Partner Agencies must accurately capture program entry and exit dates in order to ensure the integrity of client information.

Access to Client Records

Only staff who work directly with clients or who have administrative responsibilities will receive authorization to look at, enter, or edit client records.

No Client record will be shared electronically with another agency without written or verbal client consent.

A Client has the right to not answer any question and may not be denied service as a result, unless entry into a service program requires it.

A Client has the right to review the contents of their record, know who has viewed and edited it, and to request correction of inaccuracies.

Computer Crime

Partner Agencies must comply with relevant state and federal laws. These include but are not limited to those regarding: unauthorized disclosure of data, unauthorized modification or destruction of data, programs, or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both. The Homeward Authorized Agent staff and authorized agencies must comply with license agreements for copyrighted software and documentation. Licensed software must not be copied unless the license agreement specifically provides for it.

End User Ethics

Users are licensed to use the HCIS for the legitimate business purposes of a Partner Agency and in the interests of their Clients. Users may not use the HCIS for personal purposes, to defraud any entity, or to conduct any illegal activity. Minimal precautions to secure client data include the protection of usernames and passwords, maintenance of anti-virus software, and proper storage or disposal of all documents containing personally identifying information.

Resources

This Document is based with permission on the University of Massachusetts Boston's "CSPTech Policies and Procedures."

Section 1: Contractual Requirements and Roles

1.1 HCIS Governing Structure and Management

Policy: Homeward shall manage the structure that supports the operation of HCIS.

HCIS is currently used in multiple CoCs. Given the regional nature of the system, structures are in place to support shared decision-making and collaboration among CoCs.

Each CoC may have its own structure in place for managing and paying for user licenses. The HMIS lead for each CoC may require its own application for an HCIS license and may choose to subsidize user licenses. Both the application process and funding for subsidies are at the sole discretion of the HMIS lead.

HCIS Policies Committee

The HCIS Policies Committee is responsible for providing information and guidance to the Greater Richmond CoC and other CoCs related to the implementation of HCIS. The committee ensures that all HUD funded organizations are trained in and fully utilizing HCIS. This committee provides input, oversight, and guidance on the development of HCIS policies and procedures and ensures that the implementation meets or exceeds all federal and applicable regulations.

Members of the HCIS Policies Committee include representatives of all CoCs in our multi-region implementation. Each year, the HCIS Policy Committee Chair(s) will recommend a slate of members to the GrCoC Board and other applicable CoC Boards for approval. All committee members will be approved by the GRCoC board (and by other CoC boards, if applicable). The vote to approve Committee members can be conducted by email and requires a simple majority.

The responsibilities of this committee include:

1. Providing information and guidance to the Greater Richmond CoC and other CoCs as requested related to the implementation of HMIS and the designation of an HMIS Lead;
2. Ensuring compliance with HUD's data standards;
3. Providing oversight to the funding and operations of HMIS as part of the CoC;
4. Preserving data quality;
5. Ensuring that all HUD funded organization are trained in and fully utilizing HMIS;
6. Provide input, oversight, and guidance on the development of HCIS policies and procedures; and,
7. Conducting the Annual Homeless Assessment Report (AHAR).

Generally, the development of policies that will affect all CoCs would go through the HCIS Policies committee. These policies would then need to be agreed to or ratified by each of the CoCs in the implementation, if applicable.

Homeward Staff

Homeward staff is responsible for oversight of all day-to-day operations including: technical infrastructure; planning, scheduling, and meeting HCIS project objectives;

supervision of project staff, including reasonable divisions of labor; and hiring project staff.

In addition, staff (which includes the HCIS Director and the HCIS Training and Support Manager) responsibilities include:

1. Managing the relationship with the HMIS vendor
2. Providing leadership for technical strategy planning and quality assurance
3. Providing business integration services to social services agencies
4. Working with and supporting HCIS staff in other CoCs
5. Assisting agencies and CoCs with HMIS funding requests
6. Implementing HCIS to Virginia service providers
7. Managing other project resources
8. Monitoring data quality and security
9. Serving as System Administrator
   (a) Ensuring the HCIS database meets required levels of data integrity
   (b) Managing the HCIS configuration and screen layouts
   (c) Assisting users in generating required reports or helping them contract with other resources to create reports
   (d) Monitoring data quality and security
   (e) Working with agencies to close projects and redistribute licenses when necessary
10. Managing training activities
   (a) Creating training materials
   (b) Scheduling and conducting training classes
   (c) Providing one-on-one training as needed
   (d) Providing end-user support
   (e) Monitoring data quality and security
   (f) Analyzing the HCIS problem log to evaluate the need for additional training.

HCIS Administrators Group

The HCIS Administrators Group includes staff who help administer HCIS in each of the CoCs. The group meets on a monthly basis. The purpose of the group is to share ideas and information, discuss how to address challenges, and strategize about the overall administration of the system.

1.2 HCIS Contract Requirements

Policy: Homeward shall provide HCIS technical assistance to Partner Agencies.

Homeward is committed to providing quality service to existing and new participating agencies. All existing and new agencies participating in the HCIS will have user licenses and technical assistance covered under current or new contracts. Please note: Partner Agencies are responsible for all costs associated with hardware acquisition and maintenance, personnel, data entry, and internet access.

1.3 Data Analysis

Policy: Homeward shall be responsible for aggregate HCIS Data Analysis on an ongoing basis

Data analysis is as follows:

(a) Providing data quality reports for partner programs on a regular basis.

(b) Providing agency or CoC ad hoc reports on a contract basis.

(c) Providing aggregate non-identifiable data statistics for regional reporting including to HUD.

(d) Providing data analysis services to partner agencies and CoCs on a contract basis.

1.4 Systems Administration, Security, and User Accounts

Policy: System Security and Integrity shall be reviewed on a regular basis.

Homeward contracts with WellSky for hosting of the HCIS application and database. WellSky reviews all network and security logs regularly and advises the HCIS Director of any required actions. Homeward has overall responsibility (both technical and procedural) for the security of the system. All System Administrator accounts are the responsibility of Homeward. The Agency Administrator is responsible for maintenance of User accounts at the Partner Agency.

1.5 Agency Executive Director

Policy: The Executive Director of each Partner Agency shall be responsible for agency staff that has access to the HCIS.

The Executive Director of each Partner Agency is responsible for oversight of agency staff that has access to system software. The Executive Director holds final responsibility for the adherence of his or her agency's personnel to the Policies and Procedures outlined in this document and the User Responsibilities and Ethics.

The Executive Director agrees to authorize HCIS access only for staff having a legitimate business purpose for such access.

Acting on behalf of the Partner Agency, the Executive Director will:

(a) Establish business controls and practices to ensure organizational adherence to these Policies and Procedures and the User Responsibility and Ethics signed by each user;

(b) Authorize data access to agency staff and assign responsibility for custody of the data;

(c) Assume responsibility for integrity and protection of client data entered into the HCIS;

(d) Monitor compliance and periodically review control decisions.

The Agency will ensure that the Agency and its staff fully comply with the End User Terms and these Policies and Procedures and hereby agrees to fully indemnify and hold harmless Homeward from any unauthorized use, improper use, or misuse of the software and the system by the Agency and/or its staff, or any violation of law arising out of or in connection with the acts or omissions of Agency and its staff and the Agency's participation in the HCIS.

Each Agency must ensure that each user of the software and system obtains a unique user license. Only those with a user license may access and use the software and system. Sharing of user names and passwords is expressly forbidden. In addition, each user of the software and system must agree to and sign the User Policy and Code of Ethics before accessing the system.

1.6 Agency Administrator

Policy: The Executive Director of each Partner Agency will designate an Agency Administrator to serve as lead staff and primary point of contact for HCIS-related matters.

In a Continuum of Care where the number of users is small, agencies may designate an employee of one Partner Agency to serve as Agency Administrator for several agencies.

The designated Agency Administrator holds responsibility for the administration of the system software in his or her agency. The Agency Administrator is responsible for:

(a) Implementation of data security policy and standards, including administering agency-specified business and data protection controls.

(b) Entering and updating agency information

(c) Administering and monitoring access control, including granting access for authorized persons by creating usernames and passwords;

(d) Ensuring that access to the HCIS system is granted to authorized staff members only after they have received training.

(e) Detecting and responding to violations of the Policies and Procedures or agency procedures.

Notifying Homeward staff by email of the name and access level of each User that needs to be added or deleted from the system. Agency administrators may also add or delete users themselves

1.7 End Users

Policy: Partner Agencies will allow staff an appropriate level of access as needed to pursue legitimate business purposes.

(a) Homeward agrees to authorize use of the HCIS only to users who need access to the system for technical administration of the system, report writing, data analysis and report generation, back-up administration, or other essential activity associated with carrying out HCIS responsibilities.

(b) The Partner Agency agrees to authorize use of the HCIS only to users who need access to the system for legitimate business purposes such as entering, editing or viewing client records, report writing, program administration or other essential activity associated with carrying out Partner Agency responsibilities.

(c) Users must be aware of relevant confidentiality standards and take appropriate measures to prevent unauthorized disclosure of data. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the data security policy and standards as described in these Policies and Procedures. Users are accountable for their actions and for any actions undertaken with their usernames and passwords.

(d) Each End User shall sign a User Policy and Code of Ethics prior to obtaining access to the HCIS.

1.7 HCIS Participation Requirements for New Agencies

Policy: HCIS is required for agencies receiving federal and state funds targeted to serving people experiencing homelessness. Agencies and programs primarily serving survivors of sexual and domestic violence are prohibited from using HCIS.

All who want to use this system must:

a) Meet technical requirements for using HCIS (detailed in these policies and procedures).
b) Be trained in the use of the system, including training on client privacy and confidentiality, and agree to and sign the user agreement.
c) Be a participating member of the applicable CoC.
d) Have a signed agency agreement on file with Homeward.
e) Have a valid business purpose or mission for using HCIS.
f) Be a legal entity that exists (at least in part) to address homelessness.
g) Be a nonprofit or government entity.

Some who use the system receive state or federal funding that requires participation in HCIS.

For agencies that are not required to use HCIS by their funder, we may require a probationary period of six months to ensure that the system is being used as intended. Also, any agencies not funded by the state (DHCD) or federal government (HUD) should:

a) Provide a description of how it will meet the technical requirements necessary to use HCIS.
b) Describe the purpose for using HCIS and the specific projects to be tracked in the system.
c) Describe organizational policies re: client confidentiality and privacy, particularly as they relate to social media.

Applications from agencies that are not required to use HCIS will be reviewed by the HCIS policies committee and recommended for approval/disapproval to the appropriate CoC Board. The CoC Board has final decision-making authority on approval/disapproval. If any agency disagrees with the CoC Board's decision, it can appeal to the Board and provide additional information to support its case. If the appeal is unsuccessful, an agency not required to use HCIS can re-apply in six months following the same procedures outlined above.

Section 2: Participation Requirements & Privacy Plan

2.1 System and Technical Considerations

2.1.1 System Requirements

Policy: Each computer accessing the HCIS shall meet Minimum System Requirements as follows. Each computer:

(a) Must run Windows XP, Vista, Windows 7, Windows 8, or Windows 10;

(b) Must have a keyboard, mouse, and a standard SVGA monitor;

(c) Must have an internet connection meeting requirements set forth in Section 2.1.3 Implementation Connectivity;

(d) Must authenticate users using a unique user name and password;

(e) Must have self-updating anti-virus software protection installed and active;

(f) Must have an active locking screensaver; and

(g) Must be protected by a firewall (which may be hardware or software installed on a network or server).

2.1.2 Information Security Protocols

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

At a minimum, a Partner Agency must develop rules, protocols or procedures to address each of the following:

(a) Assignment of user accounts;

(b) Unattended workstations;

(c) Physical access to workstations;

(d) Policy on user account sharing;

(e) Client record disclosure;

(f) Report generation, disclosure and storage.

Information Security Protocols or procedures will protect the confidentiality of the data and to ensure its integrity at the site, as well as the confidentiality of the clients.

2.1.3 Implementation Connectivity

Policy: Each Partner Agency is required to obtain an adequate Internet connection.

An adequate internet connection is defined as a minimum of 128 KBPS, DSL, or Cable connection. Proper connectivity ensures proper response time and efficient system operation of the HCIS. Homeward staff will advise Partner Agencies on the procurement of adequate services upon request. Obtaining and maintaining an Internet connection with minimum 128 KBPS is the responsibility of the Partner Agency.

2.1.4 Maintenance of Onsite Computer Equipment

Policy: Each Partner Agency shall maintain onsite computer equipment.

Partner Agencies commit to a reasonable program of data and equipment maintenance in order to sustain an efficient level of system operation and maintain the technical standards set forth in Section 2.1 System Requirements.

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

(a) Partner Agency is responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for the utilization of the HCIS.

(b) Homeward staff members are not responsible for troubleshooting problems with Internet Connections.

(c) The Partner Agency agrees to only download and store data in a secure format.

(d) The Partner Agency agrees to dispose of documents that contain identifiable client level data by shredding paper records, deleting any information from diskette before disposal, and deleting any copies of client level data from the hard drive of any machine before transfer or disposal of property. Homeward staff is available to consult on appropriate processes for disposal of electronic client level data.

2.2 Privacy Plan

2.2.1 Agency Participation Requirements

Policy: Each Partner Agency shall comply with the following Participation Requirements:

(a) The Agency shall utilize the HCIS for legitimate business purposes only and will use Client information as needed to assist in providing adequate and appropriate services;

(b) The Agency shall consistently enter information into the HCIS and endeavor to keep information up to date;

(c) The Agency will participate in evaluation efforts to improve and refine the HCIS;

(d) The Agency shall not use the HCIS database with intent to defraud federal, state, or local governments; individuals or entities; or to conduct any illegal activity;

(e) Unless the Agency does not share information about Clients with Partner Agencies, the Agency will attempt to obtain a verbal or written Release of Information from each Client that enables Client data to be shared electronically with other Partner Agencies in the HCIS;

(f) The Agency agrees to enter no less than the minimum data elements as outlined by Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice for each Client entered;

(g) The Agency shall ensure that any person issued a User ID and password for the HCIS receive client confidentiality training and have signed a User Policy and Statement of Ethics;

(h) The Agency shall follow, comply with, and enforce the User Policy and Code of Ethics.

2.2.2 Confidentiality and Informed Consent

Policy: Each Partner Agency shall uphold standards of data confidentiality and obtain informed consent before client data is entered into HCIS.

(a) Partner Agencies must uphold federal and state confidentiality regulations to protect client records and privacy.

(b) Partner Agencies must post the HCIS Client Privacy Notice at each desk (or comparable location), and a current version of the Privacy Notice must be provided on the Agency's website (if applicable).

(c) Partner Agencies must obtain a written or verbal Release of Information to share data electronically with Partner Agencies in HCIS. Users at Partner Agencies must be prepared to explain the terms of the Release of Information and answer client questions about how their information is collected, shared, and used.

(d) Partner Agencies must allow an individual to inspect and to have a copy of any personally identifying information about the individual and offer to explain any information the individual may not understand. Agencies must then consider any request by the individual for correction of inaccuracies or incompleteness in their personally identifying information, but Agencies are not required to remove any information and may, alternatively, mark information as inaccurate or incomplete, supplementing it with additional information.

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

2.2.3 Additionally Protected Data

Specific health information (including medical diagnoses and condition details) is typically not collected by providers, but if it is, it is automatically treated as confidential with access restricted to the originating agency. Some providers (e.g., providers of Housing Opportunities for Persons with AIDS) may choose to restrict all client sharing of information by not completing a Release of Information for any clients. Domestic violence

victim service providers are prohibited from entering data into HCIS, and legal service providers are not to enter confidential client notes into HCIS.

2.2.4 Minimum Data Elements

Policy: Each Partner Agency shall input Minimum Data Elements as defined by the Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice for each client entered**.**

Partner Agencies that collect client data through the HCIS will endeavor to collect, at a minimum, the universal data elements and applicable program-specific data elements set forth in the 2014 HMIS Data Standards published by HUD. Partner Agencies may develop independent methods to gather this data.

Section 3: Training

3.1 Training Schedule

Policy: Homeward shall maintain an HCIS training schedule.

Homeward staff will publish a schedule for training and will offer education regularly. Each Continuum of Care will sign an annual contract that specifies the number of trainings to be offered in the Continuum. If no such arrangement is made, or additional training is required, training sessions can be scheduled as needed. Training sessions include 8 hours of training split over two consecutive days. Homeward recommends at least two training sessions per year. Partner Agencies are asked to RSVP for all training.

3.2 User, Administrator, and Security Training

Policy: Each HCIS User must receive appropriate training from Homeward staff.

Each User must receive HCIS training from Homeward staff before being granted access to the live system. Agency Administrators must attend an Agency Administrator training offered by Homeward in addition to User training. Partner Agencies will be notified of scheduled training sessions.

Section 4: Security Plan (User, Location, Physical and Data Access)

4.1 Access Privileges to System Software

Policy: Each Partner Agency shall adhere to standard procedures in requesting and obtaining system access.

Partner Agencies will apply the user access privilege conventions set forth in this procedure. Allocation of user access accounts and privileges will be made according to the format specified in this procedure:

(a) User access and user access levels will be determined by the Executive Director of the Partner Agency in consultation with the Agency Administrator. The Agency

Administrator will generate user names and passwords within the administrative function of the HCIS.

(b) The Agency Administrator will create all usernames using the first initial of first name and last name format. For example, John Doe's username would be JDoe. Where two Users share the same first initial and last name, Agency Administrators should use a sequential number, middle initial, or combination of these to generate a unique user name. (For example, John Edgar Doe and Jane Smith Doe could be JDoe1 and JDoe2, or JEDoe and JSDoe).

(c) Passwords are automatically generated from the system when a user is created. Agency Administrators will communicate the system-generated password to the user.

(d) The user will be required to change the password the first time they log onto the system. The password must be between 8 and 16 characters and contain 2 numbers.

(e) Passwords expire every 45 days, after which time Users are asked to choose a new password.

(f) The Agency Administrator shall terminate the rights of a user immediately upon termination from their current position. If a staff person is to go on leave for a period of longer than 45 days, their password should be inactivated within 3 business days of the start of their leave. The Agency Administrator is responsible for removing users from the system and informing Homeward of their departure.

4.2 Access Levels for System Users

Policy: Users shall be assigned an access level appropriate to their role and authority within the Partner Agency.

Partner Agencies will manage the proper designation of user accounts and will monitor account usage. The Partner Agency agrees to apply the proper designation of user accounts and manage the use of these accounts by Partner Agency staff. It is the responsibility of the Agency Administrator to create and de-activate User accounts as needed.

There are nine (9) levels of access to the HCIS system detailed in

Appendix I: Service Point Access Matrix. The level of access granted to a User should be reflective of the access a user has to client level paper records and access levels should be need-based. Need exists only for those staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.

4.3 Access to Data

Policy: Partner Agencies shall enforce the user access privileges to the system data server.

The user access privileges to the system data server are as stated below:

(a) **User Access**: Users will only view the data entered by users of their own agency unless they are sharing a client with another Partner Agency.;

(b) **Raw Data**: Users who have been granted access to the HCIS Report Writer tool have the ability to download and save client level data onto their local computer. Once this information has been downloaded from the HCIS server in raw format to an agency's computer, this data then becomes the responsibility of the agency. A Partner Agency should develop protocol regarding the handling of data downloaded from the Report Writer;

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

(d) **Access to Community and Regional Data**: Access will be granted based upon policies developed by Homeward.

4.4 Access to Client Paper Records

Policy: Partner Agencies shall establish procedures to handle access to client paper records.

These procedures will:

(a) Identify which staff has access to the client paper records and for what purpose. Staff should only have access to records of clients, which they directly work with or for data entry purposes;

(b) Identify how and where client paper records are stored;

(c) Develop policies regarding length of storage and disposal procedure of paper records;

(d) Develop policies on disclosure of information contained in client paper records.

4.5 Physical Access Control

Policy: Each Partner Agency shall adhere to Physical Access Control Procedures.

Physical access to the system data processing areas, equipment, and media must be controlled. Access must be controlled for the transportation of data processing media and other computing resources. The level of control is contingent on the level of risk and exposure to loss. Personal computers, software, documentation, and storage media (e.g., CDs, zip drives) shall be secured proportionate with the threat and exposure to loss. Available precautions include equipment enclosures, lockable power switches, equipment identification, and fasteners to secure the equipment.

(a) Homeward staff with the Agency Administrators within Partner Agencies will determine the physical access controls appropriate for their organizational setting based on the HCIS security policies, standards, and guidelines;

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

(c) Printed versions of confidential data should not be copied or left unattended and open to unauthorized access;

(d) Media containing client-identified data will not be shared with any agency other than the owner of the data for any reason. HCIS data may be transported by authorized employees using methods deemed appropriate by the Partner Agency that meet the above standard. Reasonable care should be used, and media should be secured when left unattended;

(e) Magnetic media containing HCIS data that is released and or disposed of from the Partner Agency should first be processed to destroy any data residing on that media;

(f) Degaussing and overwriting are acceptable methods of destroying data;

(g) Responsible personnel must authorize the shipping and receiving of magnetic media, and appropriate records must be maintained;

(h) HCIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

4.6 Unique User Identification (ID) and Password

Policy: Each User shall be granted a unique user ID and password.

Only authorized users will be granted a user ID and password to ensure that only authorized users will be able to enter, modify, or read data.

(a) Each user will be required to enter a unique user ID with a password in order to logon to the system;

(b) User ID and passwords are to be assigned to individuals;

(c) The user ID will be the first initial and full last name of the user. Where two users share the same first initial and last name, Agency Administrators should use a sequential number, middle initial, or combination of these to generate a unique user name. (For example, John Edgar Doe and Jane Smith Doe could be JDoe1 and JDoe2, or JEDoe and JSDoe);

(d) The password must be no less than eight and no more than sixteen characters in length;

(e) The password must be alphanumeric and contain 2 or more numbers;

(f) Discretionary Password Reset - Initially each user will be given a password for one time use only. The first or reset password will be automatically generated by the HCIS and will be issued to the user by the Agency Administrator. Homeward staff is also available to agency staff to reset passwords. Because users must immediately change their assigned passwords, passwords may be communicated verbally or through email.

(g) Forced Password Change (FPC): FPC will occur every forty-five days once a user account is issued. Passwords will expire and users will be prompted to enter a new password. Users may not use the same password consecutively, but may use the same password more than once.

(h) Unsuccessful Logon: If a user unsuccessfully attempts to logon three times, the user ID will be "locked out," and access to the system will be revoked until the user logs in with a new password.

(i) Access to computer terminals within restricted areas should be controlled through a password or through physical security measures;

(j) Each user's identity should be authenticated through an acceptable verification process;

(k) Passwords are the individual's responsibility, and users cannot share passwords;

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

4.7 Right to Deny User and Partner Agency's Access

Policy: Violations of security protocols shall result in denial of access to the HCIS.

A Partner Agency or an individual user may have system access suspended or revoked for violation of the security protocols. Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access.

(a) Homeward will investigate all reported and potential violations of security protocols.

(b) Homeward shall notify the Agency Administrator within one business day of any such suspension or revocation of access, the reason or reasons for such action, and the party responsible for further investigation of the issue.

(c) Any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include, but are not limited to: a formal letter of reprimand, suspension of system privileges, revocation of system privileges, or criminal prosecution.

4.9 Data Access Control

Policy: Partner Agencies and Homeward staff shall monitor access to system software.

Agency Administrators at Partner Agencies and Homeward staff will regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access. Agency Administrators at Partner Agencies and Homeward staff must implement discretionary access controls to limit access to HCIS information when available and technically feasible. Partner Agencies and Homeward staff must audit all unauthorized accesses and attempts to access HCIS information.

4.10 Auditing: Monitoring and Violations

Policy: Homeward staff will monitor access to systems that could potentially reveal a violation of information security protocols.

Violations will be reviewed for appropriate disciplinary action that could include license revocation or criminal prosecution.

All exceptions to these standards are to be requested in writing by the Executive Director of the Partner Agency and approved by the Executive Director of Homeward as appropriate. Monitoring shall occur as follows:

(a) Monitoring compliance is the responsibility of Homeward;

(b) All users and custodians are obligated to report suspected instances of noncompliance;

(c) Homeward staff will review potential security violations and require or recommend corrective or disciplinary action to the agency;

(d) Users should report security violations to the Agency Administrator, and the Agency Administrator will report to Homeward staff.

(e) Should there be a violation by the Agency Administrator, users should report directly to Homeward staff.

4.11 Local Data Storage

Policy: Client records containing identifying information that are stored within the Partner Agency's local computers are the responsibility of the Partner Agency.

Partner Agencies should develop policies for the manipulation, custody, and transmission of client-identified data sets. A Partner Agency will develop policies consistent with Information Security Policies outlined in this document regarding client-identifying information stored on local computers.

Note: Services provided through Wellsky for hosting of the HCIS application and database also include a Disaster Recovery Plan providing for nightly backups and offsite storage.

4.12 Transmission of Client Level Data

Policy: Client level data will be transmitted in such a way as to protect client privacy and confidentiality.

Administrators of the system server data must be aware of access-control vulnerabilities for that data while they are in transmission within the network. Transmission will be secured by 128-bit encryption provided by SSL Certificate protection, which is loaded at the HCIS server.

4.13 Compliance and Monitoring

Policy: Agencies and users must help ensure the security, privacy, and confidentiality of client data.

In December 2011, the U.S. Department of Housing and Urban Development released a proposed rule to establish regulations for HMIS, which is the currently prevailing set of regulations governing HMIS operations. (Federal Register, Vol. 76, No. 237, pages 76917 – 76927.) The HEARTH Act (2009) required HUD to ensure the operation of and consistent participation in HMIS. The HEARTH Act codified the Continuum of Care planning process and certain data collection requirements as well as operation of and participation in HMIS for certain funded programs and agencies.

The CoC is responsible for ensuring that the HMIS for the Continuum of Care (CoC) is operated in accordance with the provisions of the new regulations and other applicable laws. The HMIS Lead is responsible for developing written policies and procedures for all agencies using HMIS by executing a participation agreement and monitoring compliance. Governing policies and procedures must provide for the security, confidentiality, and privacy of data

.

Established in July 2013, the HMIS Policies Committee is responsible for providing information and guidance to the Greater Richmond CoC and other CoCs and Local Planning Groups (LPGs) related to the implementation of HMIS. This committee will ensure that all HUD funded organizations are trained in and fully utilizing HMIS. This committee will provide input, oversight, and guidance on the development of HMIS policies and procedures and ensure that all CoCs and LPGs covered in this implementation of HMIS meet or exceed all federal and applicable regulations.

HUD regulations lay out a number of requirements for CoCs, HMIS Leads, and agencies participating in HMIS. In addition to the technological requirements for HMIS participating agencies (laid out in the Policies and Procedures document), there are a number of requirements for HMIS participating agencies to ensure the security, privacy, and confidentiality of client data.

As laid out in the Policies and Procedures and other approved HMIS documents, the requirements for compliance with HMIS are as follows:

- Meeting or exceeding technical and system requirements
- Participation in training for users according to level of access
- Complying with the User Policy and Code of Ethics
- Execution of signed participation agreements
- Complying with the policies and procedures and data quality standards set forth in the Policies and Procedures document not otherwise specified.

All users of HMIS agree to notify a System Administrator, the HMIS Lead, or LPG or CoC leadership of violations of the policies and procedures or User Policy and Code of Ethics. Additionally, HMIS Lead staff and/or System Administrators may identify lack of compliance during the provision of services and training related to HMIS. Finally, the HMIS Policies Committee may develop additional monitoring processes and request additional reports from the HMIS Lead concerning progress toward full compliance by all users or agencies.

For violations of compliance that threaten the HMIS implementation as a whole (e.g. violations of client or system data, sharing of licenses, failure to signed written agreements as required in 24 CFR 580.9), usage of HMIS will be immediately revoked or require a plan to rectify the lack of compliance within 48 hours upon agreement with the HMIS Lead in consultation with the relevant CoC or LPG leadership. The HMIS Lead will then notify HUD, DHCD, and other relevant funders of the change in usage status.
For violations of compliance that do not pose an immediate threat to the privacy, security, or confidentiality of client or system data (e.g., not meeting the timeliness standard for data entry), the participating agency may seek a waiver of the standard from the HMIS Policies Committee in consultation with the HMIS Lead. If a waiver is not granted, the

agency found to be out of compliance will receive a written warning from the HMIS Lead and asked to develop a plan to rectify the lack of compliance within 7 business days. If an agency continues to be out of compliance, the HMIS Policies Committee will review the matter and make a recommendation for a sanction.

Agencies participating in HMIS with concerns about the sanctions process including waivers may file an appeal with the relevant CoC board or LPG. The notice of appeal must include a written statement specifying in detail all grounds asserted for the appeal. The appeal must be submitted by an individual authorized to represent the agency and must include the specific sections of the compliance process on which the appeal is based. The CoC or LPG leadership will review the appeal in consultation with the HMIS Policies Committee and the HMIS Lead and notify the appealing agency of its decision.
All eligible appeals will be read, reviewed, and evaluated by the CoC or LPG leadership within 48 hours of the appeal. The CoC or LPG leadership will provide a determination of the appeal to the appealing applicant and the HMIS Policies Committee. The recommendation of the CoC or LPG leadership will be final. A written summary of the CoC or LPG leadership decisions will be provided to the appealing agency.

Section 5: Technical Support and System Availability

5.1 Planned Technical Support

Policy: Homeward staff shall offer technical support to all Partner Agencies on use of the system software.

Homeward staff will assist agencies in:

(a) Start-up and implementation;
(b) On-going technical assistance;
(c) Training;
(d) Technical assistance with report writing and any other additional modules.

5.2 Partner Agency Service Request

Policy: Homeward staff shall respond to requests for services.

All Users may make service requests. The preferred method of sending a request in through the helpdesk email: hcis@homewardva.org, and Users may also call HCIS staff for assistance. The advantage of using the helpdesk email is that all staff have access to it, so they can respond more quickly to User needs.

5.3 Hours of System Operation

Policy: System shall be accessible 24 hours a day 7 days a week with the exception of a weekly routine maintenance window of a two hour duration. At present, this maintenance window is identified for Wednesday evenings from 5:00 to 7:00 p.m.

The system will be available to the community of users in a manner consistent with the user's reasonable usage requirements.

5.4 Planned Interruption to Service

Policy: Homeward staff shall inform Partner Agencies of any planned interruption to service except for routine maintenance as described in 5.3 Hours of System Operation.

Partner Agencies will be notified of planned interruption to service one (1) week prior to the interruption. Homeward staff will notify Partner Agencies via e-mail the schedule for the interruption to service. An explanation of the need for the interruption will be provided and expected benefits or consequences articulated. Homeward staff will notify Partner Agencies via e-mail that service has resumed.

5.5 Unplanned Interruption to Service

Policy: Homeward shall notify each Partner Agency of unplanned interruption to service in a timely manner.

Partner Agencies may or may not be notified in advance of unplanned interruption to service. Partner Agencies will be notified of unforeseen interruption to service that are expected to exceed two (2) hours. When an event occurs that makes the system inaccessible, Homeward staff and Wellsky may make a determination to switch service to the secondary server. At this point, users will be able to resume operation. The procedure will be as follows:

(a) Event is detected;
(b) Analyzed;
(c) Repair the problem within two (2) hours or switch to secondary server;
(d) Resume operation at Partner Agency.

When production server becomes available:

(a) During the next full backup process, production server will be restored with latest data from secondary server;
(b) Homeward staff will notify via e-mail that service has resumed;
(c) Return to normal operation.

Section 6: HUD Resources

6.1 HUD Data and Technical Standards

HUD publishes data and technical standards to ensure that data that is required to fulfill HUD reporting requirements is collected in a consistent manner and that privacy and security of client information is protected. Currently applicable standards are:

- The July 2004 Data and Technical Standards Final Notice (FR 4848-N-02 – available at

https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf.)

- The March 2010 Homeless Management Information System (HMIS) Data Standards – Revised Notice (available at http://www.hudhre.info/documents/FinalHMISDataStandards_March2010.pdf)
- The August 2014 HMIS Data Standards Manual (available at https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf.)

In addition, the HMIS proposed rule (available at https://www.onecpd.info/resources/documents/HEARTH_HMISRequirementsProposedRule.pdf) published in December 2011 is currently under revision and is not currently in effect. Basically, the proposed rule includes 1) uniform technical requirements of HMIS; 2) proper collection of data and maintenance of the database; and 3) confidentiality of the information in the database.

For 2017, the 2017 HMIS Data Standards Manual was issued, effective October 1, 2017, and available here: https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual-2017.pdf.

For 2016, critical changes were incorporated into the 2014 HMIS Data Standards Manual available here: https://www.hudexchange.info/resource/3824/hmis-data-dictionary/.

For 2015, critical changes were announced and described here: https://www.hudexchange.info/news/hud-releases-critical-changes-to-the-2014-hmis-data-standards/; however the link to the data manual does not currently work (as of July 7, 2017).

Appendix I: Service Point Access Matrix

ServicePoint® User Roles Version 5.11 September 5, 2014	Resource Specialist II	Case Manager I	Case Manager II	Case Manager III	Agency Admin	Read Only III	System Admin I	System Admin II
ClientPoint								
View client record		X	X	X	X	X	X	X
View inactive client record								X
Modify client record		X	X	X	X		X	X
Delete client record					X		X	X
Delete any client record								X
Ability to modify static client security		X	X	X	X		X	X
Ability to modify dynamic client security		^	^	^	^		^	X
View client releases of information		X	X	X	X	X	X	X
Modify / delete client releases of information		X	X	X	X		X	X
View case managers		X	X	X	X	X	X	X
Modify / delete case managers		X	X	X	X		X	X
View Assessments Tab		X	X	X	X	X	X	X
Add/Edit client answers In Assessment Tab		X	X	X	X		X	X
View Case Plans Tab		X	X	X	X	X	X	X
Add/Edit goals, case notes, action steps Case Plans		X	X	X	X		X	X
View client incidents		X	X	X	X	X	X	X
Modify / delete client incidents			X	X	X		X	X
View client needs/services/referrals		X	X	X	X	X	X	X
Modify / delete client needs/services/referrals		X	X	X	X		X	X
View client entry/exits		X	X	X	X	X	X	X
Modify / delete client entry/exits		X	X	X	X		X	X
View client file attachments		X	X	X	X	X	X	X
Modify / delete client file attachments		X	X	X	X		X	X
Delete Households								X
Delete Households (with restrictions)*		X	X	X	X		X	
ResourcePoint	X	X	X	X	X	X	X	X
ShelterPoint								
CommunityPoint								
Global Action given to users in order to disable/hide admin areas which should not be accessible	X							

ServicePoint® User Roles Version 5.11 September 5, 2014	Resource Specialist II	Case Manager I	Case Manager II	Case Manager III	Agency Admin	Read Only III	System Admin I	System Admin II
CallPoint								
Modify Call Records		X	X	X	X		X	X
View Call Records		X	X	X	X		X	X
View Inactive Call Records								X
Reports								
Ability to view the reports tab and run reports		X	X	X	X		X	X
Enable the ability to generate system-wide reports								X
Enable ability to delete subordinate or parent provider ReportWriter reports								X
Audit Reports								
Audit Report					X		X	X
User information					X		X	X
User Login					X		X	X
Audit Access Report								X
Provider Reports								
AHAR Report					X	X	X	X
Call Record Report		X	X	X	X	X	X	X
Client Served Report		X	X	X	X	X	X	&
Client Intake Report					X		X	X
Daily Unit Report		X	X	X	X	X	X	X
Duplicate Client Report						X		X
Entry/Exit Report		X	X	X	X	X	X	&
ESG Caper Report		X	X	X	X	X	X	&
PATH Report		X	X	X	X	X	X	&
Referrals Report		X	X	X	X	X	X	X
Service Transaction Report		X	X	X	X	X	X	X
Needs Report		X	X	X	X	X	X	&
Report/Writer								
FundManager								
Modify the Provider Preferences controlling FundManager Fund/Vendor creation							X	X
Full control in the FundManager module								X
Create/modify legacy-style, limited Funds based on the legacy Funding Sources Picklist							X	X
Access to FundManager module, even if User is not a Review Agent or Fund Administrator					X		X	X

ServicePoint® User Roles Version 5.11 September 5, 2014	Resource Specialist II	Case Manager I	Case Manager II	Case Manager III	Agency Admin	Read Only III	System Admin I	System Admin II
Administration								
Add / edit / delete users					@		X	X
View users					@		X	X
View Inactive Users							X	X
Reset bad login attempts for users					@		X	X
Reset Passwords					@		X	X
Able to assign resource groups to users					@		X	X
Add Provider							X	X
Edit Provider	#				#		X	X
Delete Provider	%				%		X	X
View inactive providers								X
Modify Provider Visibility information					X		X	X
Modify Provider Services in Provider Admin	@				X		X	X
Modify Provider Profile information	X				X		X	X
View Provider Maintenance information	X				X		X	X
Modify Provider Maintenance information	X				X		X	X
Add Subordinate Providers	X				X		X	X
Modify Provider Configuration information	X				X		X	X
View Provider Configuration information	X				X		X	X
View Provider Display Settings	X				X		X	X
Modify Provider Display Settings	X				X		X	X
Add / edit / remove agency news	X	X	X	X	X		X	X
Add / edit / remove system news							X	X
Access to Create / Read / Update / Delete assessment information. User can change settings							X	X
Access to AIRS Taxonomy Admin							X	X
View Picklists							X	X
Modify Picklists							X	X
Purchase licenses							X	X
Allocate and assign licenses					X		X	X
Shadow Mode					X		X	X
View resource groups							X	X
Add / edit / delete resource groups							X	X
View reporting groups					X		X	X
Add / edit / delete reporting groups					X		X	X
View visibility groups					X		X	X
Add / edit / delete only local visibility groups					X		X	
Add / edit / delete all visibility groups								X
View EDA groups					X		X	X
Add / edit / delete EDA groups					X		X	X
Send system emails (using Email Admin)	X				X		X	X
View System Preferences							X	X
Modify System Preferences							X	X
Access to Measurements Admin							X	X
Access to review records in Provider Approval Bin							X	X
Other								
Export of Providers							X	X
Provider Admin sections disabled when the provider is outside the current provider's tree								
Bypass Security For the current tree (same as agency-admin bypass in SP v3&4)				X	X		X	
Bypass Security						X		X
Bypass Release of Info							X	X
Delete any assessment data system-wide								X
Enter Data As other users		X	X	X	X		X	
Enable Backdate Mode	^	^	^	^	^		^	^
Backdate Release of Info		X	X	X	X		X	X
System Support								
Generate XML Exports								X

X: Users have access to this section of *ServicePoint or* **@:** Users have access to this section for only their provider or EDA provider.

* A) when household is NOT used by the providers outside of the user's provider or providers in the user's Enter Data As (EDA) list*, and the house

B) When the household IS used but only by the user's provider or providers in the user's EDA list*, and the household does NOT contain clients w

%: Users can neither delete the Provider they belong to, nor any of their Parent Providers.

#: Users cannot edit their Parent Provider, they may edit their own provider or their Subordinate Providers Only.

^: Action can be done only ***If allowed in the user permissions***

&: Users can run the report for Provider Groups.

Appendix II: Data Quality and Monitoring Plan

Homeward worked with representatives from the CoCs that are a part of its multi-site HMIS implementation to develop appropriate data quality standards. As a part of this process, staff reviewed HUD guidelines and data quality recommendations, as well as plans from other communities.

This plan details the minimum data quality standards, as well as a monitoring plan that describes how data quality will be assessed on a quarterly basis.

Data Quality Plan

Components of a data quality plan should include timeliness; completeness of data, clients served, and bed utilization; accuracy and consistency; monitoring; and incentives and enforcement (HUD HMIS TA Initiative, 2009). These components are addressed below.

Timeliness

Policy: All universal data elements should be collected on all clients at intake. Information should be entered into HCIS within an appropriate number of days (by program type). Complete and accurate data for the quarter must be entered into HCIS by the 15th of the following month (i.e., April 15 for Q1, July 15 for Q2, October 15 for Q3, and January 15 for Q4).

Purpose: Data in HCIS needs to be up to date in order to ensure timely and accurate reporting. Minimizing the amount of time between intake/data collection and data entry increases accuracy and provides opportunities for follow up if additional information is needed.

Proposed standards: The table below describes standards for entering client records. Note that there may be other standards required by funders (e.g., recertifications of information). Note that data timeliness standards differ depending on which CoC you are located in.

Program type	**# days for entering client records**	
	VA-513 and VA-521	VA-500 and VA-514
Coordinated assessment	3 days	Same day
Day shelter	1 week	3 days
Emergency shelter	1 week	3 days
Street outreach	1 week	3 days
Permanent housing (housing only, housing with services, and permanent supportive housing)	1 weeks	3 days
Homelessness prevention	1 week	3 days
Permanent housing – rapid rehousing	1 week	3 days
Safe Haven	1 week	3 days
Services only	1 week	3 days
Transitional housing	1 week	3 days
Other	1 week	3 days

Monitoring: Initially, average time between entry date and entry of the client record in HCIS will be monitored on a quarterly basis.

Completeness: Data

Policy: Information entered into HCIS should be truthful, accurate, and complete.

Purpose: Data that accurately describes the characteristics and needs of clients helps ensure that appropriate services and programs exist in the community. Missing data can negatively impact a provider's ability to provide appropriate services. Additionally, complete information is important for reporting purposes (including the NoFA and the AHAR) and can affect funding for the CoC and its providers.

Standard: The table below describes, by program type, the amount of allowable missing data. Note that in spite of the idea that some amount of missing data is allowed, providers will be asked to fix as much missing data as they are able to in order to facilitate accurate and complete reporting.

Overall, less than 2% missing data in any universal data element or program-specific data element field is suggested, with an exception made for outreach programs, which are expected to try to get good data from clients over time. Also note that due to the nature of Social Security Numbers, up to 5% don't know/refused is acceptable.

Program type	% allowable missing	*% allowable don't know/refused
Coordinated assessment	2%	3%
Day shelter	2%	3%
Emergency shelter	2%	3%
Street outreach	10%	10%
Permanent housing (housing only, housing with services, and permanent supportive housing)	2%	3%
Homelessness prevention	2%	3%
Permanent housing – rapid rehousing	2%	3%
Safe Haven	2%	3%
Services only	2%	3%
Transitional housing	2%	3%
Other	2%	3%

*Social Security Numbers may have higher rates of don't know/refused – up to 5%.

Monitoring: On a quarterly basis, data completeness reports will be generated for all programs that use HCIS.

Completeness: Clients Served and Bed Utilization

Policy: Accurate information should be entered in HCIS on all clients who access the homeless services system. The expectation is that all clients who receive services from a program that uses HCIS will have a corresponding record in the system.

Purpose: Not entering or exiting clients can result in inaccurate estimates of the number of clients served during a time period. In addition to ensuring that the appropriate data elements are entered, programs that serve clients in residential settings (e.g., emergency shelter, permanent housing, permanent supportive housing, Safe Haven, and transitional housing) need to keep their entry/exits up to date. High or low utilization rates can be a sign that there are problems that need to be addressed with data entry or that there are programmatic changes that need to be reflected in the system (e.g., a change in the number of available beds).

Standard: All clients should be entered into HCIS, and their records should be closed shortly upon their leaving the program.

Monitoring: On a quarterly basis, utilization rates will be provided to residential programs and open entries reports provided to other program types.

Accuracy/Consistency

Policy: Accurate information that utilizes consistent definitions is entered into HCIS.

Purpose: To ensure that data elements have a common meaning among users so that data has a consistent meaning.

Standard: All data in HCIS shall be collected and entered in a common and consistent manner across all programs. All users of the system must complete an initial training before accessing the live system. All users must recertify their knowledge of consistency practices on an annual basis. A basic intake form that collects data in a consistent manner will be available to all programs, which they can alter to meet their additional needs, provided the base document does not change.

Current HMIS Data Standards are posted on Homeward's website.

Data Quality Process/Monitoring

Policy: Programs and agencies should receive information about data quality on a quarterly basis and use this information to identify and resolve any issues.

Purpose: To ensure that the standards for timeliness, completeness, and accuracy are met and that data quality issues are identified and resolved.

Standard:

- Agencies and CoC coordinators provide timely updates to HCIS staff regarding any changes to programs (e.g., program closings, new programs, capacity).
- HCIS or CoC staff will run data quality reports on at least a quarterly basis and provide them to the agencies to review.
- Program providers will review their data and make necessary corrections to meet the above data standards.
- HCIS staff will assist providers in correcting data and updating program information as needed.

Incentives/Enforcement

Incentives and enforcement policies will be developed on a CoC level. In the Greater Richmond CoC, incentives and enforcement will be addressed as a part of the Performance Improvement committee.