

Homeward Community Information System

Policies and Procedures 3.0

Revised 1/27/14



Table of Contents

Definitions.....	3
Governing Principles.....	3
Section 1: Contractual Requirements and Roles.....	5
1.1 HCIS Governing Structure and Management	5
1.2 HCIS Contract Requirements	6
1.3 Data Analysis	6
1.4 Systems Administration, Security, and User Accounts	6
1.5 Agency Executive Director.....	7
1.6 Agency Administrator.....	7
1.7 End Users	8
Section 2: Participation Requirements.....	9
2.1 System Requirements	9
2.2 Agency Participation Requirements	9
2.3 Interagency Data Sharing	10
2.4 Confidentiality and Informed Consent.....	10
2.5 Minimum Data Elements	10
2.6 Information Security Protocols.....	11
2.7 Implementation Connectivity	11
2.8 Maintenance of Onsite Computer Equipment.....	11
Section 3: Training.....	12
3.1 Training Schedule.....	12
Section 4: User, Location, Physical and Data Access.....	12
4.1 Access Privileges to System Software	12
4.2 Access Levels for System Users	13
4.3 Access to Data	13
4.4 Access to Client Paper Records.....	14
4.5 Physical Access Control.....	14
4.6 Unique User Identification (ID) and Password.....	15
4.7 Right to Deny User and Partner Agency’s Access.....	16
4.9 Data Access Control.....	16
4.10 Auditing: Monitoring, and Violations	16
4.11 Local Data Storage	17
4.12 Transmission of Client Level Data.....	17
Section 5: Technical Support and System Availability	17
5.1 Planned Technical Support	17
5.2 Partner Agency Service Request	18
5.3 Hours of System Operation	18
5.4 Planned Interruption to Service	18
5.5 Unplanned Interruption to Service	19
Section 6: HUD Resources	20
6.1 HUD Data and Technical Standards.....	20
Appendix I: Service Point Access Matrix	21

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 Bowman Systems, Inc.

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 requirements as prescribed by 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 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 HCIS System Operation.

The Homeward Executive Director shall be the final decision makers of all policies and procedures by which the HCIS is governed. The Homeward staffing of the HCIS shall be:

- (a) HCIS Director
- (b) HCIS Training and Support Manager
- (c) Other staff as required

The HCIS management structure will adequately support the operations of the HCIS system according to the Guiding Principles described in the Introduction. The responsibilities of Homeward staff will be apportioned according to the information provided below.

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.

HCIS Director

The HCIS Director is responsible for integrating Agencies and CoC's with the regional HMIS collaborative. Responsibilities include:

1. Responsible for Bowman Systems negotiations and relationship
2. Provides leadership for technical strategy planning and quality assurance
3. Providing business integration services to social services agencies
4. Works to assist agencies and CoC's with HMIS funding requests
5. Implementing HCIS to Virginia Service Providers
6. Managing other project resources
7. Monitoring data quality and security
8. Serving as System Administrator

System Administrator

As System Administrator, the HCIS Director is responsible for overseeing usage of the HCIS application and being available for phone support as needed. Other duties are:

1. Ensure the HCIS database meets required levels of data integrity
2. Manage the HCIS configuration and screen layouts
3. Assist in generating required reports
4. Monitoring data quality and security

Training and Support Manager

The Training and Support Manager is responsible for HCIS training and support. Responsibilities include:

1. Creation of training materials
2. Scheduling and conducting training classes
3. One on one training as needed.
4. End-user Q & A support.
5. Monitoring data quality and security
6. Analyzing the HCIS problem log to evaluate the need for additional training.

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 queries 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 Bowman Systems, Inc. for hosting of the HCIS application and database. Bowman 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.
- (f) Notifying all users in their agency of interruptions in service.
- (g) Notifying the HCIS Director by letter or email of the name and access level of each User being added or removed from the system.

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.

Section 2: Participation Requirements

2.1 System Requirements

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

- (a) Must run Windows 98, ME, 2000, NT, XP, or Vista;
- (b) Must have a keyboard, mouse, and a standard SVGA monitor;
- (c) Must have an internet connection meeting requirements set forth in Section 2.7 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).

2.2 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 HMIS database with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity;
- (e) Before entering Client information into the HCIS, the Agency will obtain a Release of Information from each Client that includes permission for entry of Client data into 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 Statement of Ethics; and

- (i) Client Consent Forms must be signed by all clients to authorize the sharing of their personal information electronically with other Partner Agencies through the HCIS software system.

2.3 Interagency Data Sharing

Policy: Partner Agencies wishing to share Protected Health Information (PHI) must establish Interagency Data Sharing Agreements that meet or exceed the standards of state and federal law.

Client data that is additionally protected by state or federal law, including but not necessarily limited to: Health, Substance Abuse treatment, Domestic Violence, and Mental Health data, is automatically treated as confidential with access restricted to the originating agency. Partner Agencies that wish to share this Protected Health Information must complete and submit Interagency Data Sharing Agreements before sharing of such data is allowed. Homeward staff will assist in the preparation of these documents.

2.4 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 obtain written Client consent before entering Client data in HCIS. Users at Partner Agencies must be prepared to explain the terms of consent and/or answer Client questions about consent.
- (c) 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.

2.5 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 Minimum Data Elements set forth in the HMIS Data and Technical Standards Final Notice published in the Federal Register July 30, 2004. Partner Agencies may develop independent methods to gather this data.

2.6 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.

2.7 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.

2.8 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.

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: 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 deemed by the Executive Director of the Partner Agency in consultation with the Agency Administrator. The Agency Administrator will generate username 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 system data server.

The user access privileges to 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. Security measures exist within the HCIS software system which can restrict agencies from viewing each other's data;
- (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 diskettes 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. If a user has a first initial and last name that is identical to a user already in the system, the User ID will be the first initial and last name plus the number 1;
- (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. Passwords will be communicated in written or verbal form (not via email.) Only the first time, temporary password can be communicated via email. Homeward staff is also available to agency staff to reset passwords.
- (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 five times, the User ID will be "locked out", access permission revoked and unable to gain access until their password is reset in the manner stated above.
- (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, termination of employment and/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 termination of employment and/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 the HCIS Director;
- (b) All users and custodians are obligated to report suspected instances of noncompliance.
- (c) Homeward staff will review standards violations and require or recommend the agency through corrective and disciplinary actions;
- (d) Users should report security violations to the Agency Administrator, and the Agency Administrator will report to the HCIS Director.
- (e) Should there be a violation by the Agency Administrator, Users should report directly to the HCIS Director.

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.

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 Central 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.

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 service requests will arrive from the Agency's Executive Director or the Agency Administrator. Homeward will respond to service requests, however, Homeward staff will require that proper communication channels (phone, fax, or e-mail) be established and used at all times. To initiate a service request from a Partner Agency:

- (a) Agency Management Staff (Executive Director or Agency Administrator) contact the Homeward Training and Support Manager;
- (b) Homeward staff will determine resources needed for service;
- (c) Homeward staff will be available to the community of Users in a manner consistent with the User's reasonable service request requirements. Homeward staff are available for Technical Assistance, questions, and troubleshooting generally between the hours of 8:30 A.M.-4:30 P.M. Monday through Friday, excluding state and federal holidays;
- (d) Homeward contacts agency management staff to work out a mutually convenient service schedule.

Chain of communication:

- Agency Staff
- Agency Administrator or Executive Director
- Homeward Training and Support Manager
- HCIS Director
- Homeward Executive Director

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 2-hour duration. At present, this maintenance window is identified for Wednesday evenings from 5:00 to 7:00 PM.

The system will be available to the community of users in a manner consistent with the user's reasonable usage requirements. Members of Homeward staff agree to minimally operate the system web site twenty-four hours a day/ seven days a week, excluding acts of nature, or federal and state declared emergency situations.

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 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 Bowman Internet Systems will 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 [http://www.hmis.info/classicAsp/documents/ HUD%20Data%20and%20Technical%20Standards.pdf](http://www.hmis.info/classicAsp/documents/HUD%20Data%20and%20Technical%20Standards.pdf).)
- The March 2010 Homeless Management Information System (HMIS) Data Standards – Revised Notice (available at [http://www.hudhre.info/documents/ FinalHMISDataStandards_March2010.pdf](http://www.hudhre.info/documents/FinalHMISDataStandards_March2010.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.

Appendix I: Service Point Access Matrix

	Resource Specialist I	Resource Specialist II	Resource Specialist III	Volunteer	Agency Staff	Case Manager	Agency Administrator	Executive Director	System Operator	System Administrator I	System Administrator II
Client Point											
Profile				X	X	X	X	X		X	X
Employment						X	X	X		X	X
Residential History						X	X	X		X	X
Medical/Addiction							X	X		X	X
Legal						X	X	X		X	X
Military						X	X	X		X	X
Case Notes						X	X	X		X	X
Worksheets					X	X	X	X		X	X
Service Point											
Referrals				X	X	X	X	X		X	X
Check In/Check Out				X	X	X	X	X		X	X
Other Services					X	X	X	X		X	X
Resource Point	X	X	X	X	X	X	X	X	X	X	X
Shelter Point				X	X	X	X	X		X	X
Reports						X	X	X		X	X
Administration											
Add Users							X	X	X	X	X
Remove Users							X	X	X	X	X
Reset Password							X	X	X	X	X
Add Agency									X	X	X
Edit Agency		X	X				X	X	X	X	X
Remove Agency									X	X	X
Pick list Options									X	X	X
Licenses									X	X	X
Other Options									X	X	X