

3

Policy and Procedures

In this chapter we will define the general requirements and provide an overview of the confidentiality and privacy requirements, CHO and user requirements and system security for the HMIS system. Idaho Housing and Finance Association (IHFA) has instituted the use of ServicePoint as the HMIS system in response to the Homeless Management Information System (HMIS): Data and Technical Standards Final Notice (Federal Register Vol. 69 No. 146), which is hereby incorporated by reference. **These Policies and Procedures apply to ALL persons or organizations, using any portion of the HMIS system.**

For more information regarding HMIS Policy and Procedures, please contact the HMIS System Administrator.

- Confidentiality Requirements
- Privacy Requirements
- HMIS Use and Responsibilities
- System Security

Confidentiality Requirements

For all information entered in the HMIS system, the Covered Homeless Organization (CHO), Service Providers, Users, and Agencies are bound by all applicable federal and state confidentiality regulations and laws that protect Client records that will be accessed or entered into the HMIS system.

- HIPAA Privacy Rules take precedence over HMIS privacy standards. If an agency is a HIPAA covered agency, they must abide by HIPAA regulations.
- Rules for Domestic Violence Shelters and Service Providers take precedence over HMIS privacy standards and data entry requirements. Please contact your HMIS System Administrator for information.

The Idaho HMIS system maintains a common database with all Affiliated Service Providers which allows for the sharing of information. Some of the data HMIS collects is considered Protected Personal Information (PPI). Protected Personal Information is defined as:

Any information that can be used to identify a particular individual. Protected Personal Information includes without limitation a Client's name, Social Security Number, Date of Birth, and such personal identifying information that identifies directly, indirectly, by linking with other identifying information to identify a specific individual, or can be manipulated by a reasonably foreseeable method to identify an individual.

Unauthorized disclosure of Protected Personal Information (PPI) may be grounds for legal action.

Sharing of HMIS data among Affiliated Service Providers is encouraged but not required. Items excluded from sharing unless specifically released by the Client include medical, legal, case management and case notes, and file attachments.

Any requests for release of information, including court orders and subpoenas, shall be referred to IHFA. The Covered Homeless Organization, Users and Agencies agree not to release any confidential information received from the HMIS database to any organization or individual

Service Provider/CHO/User Responsibilities

- C.1 The Service Provider/CHO is responsible for ensuring that all staff, volunteers and other persons in their organization using or accessing information from HMIS receive confidentiality training to include HMIS use and all applicable confidentiality laws.
- C.2 The Service Provider/CHO/User shall utilize the IHFA HMIS Client Consent & Release of Information Authorization form for all Clients. The Service Provider/CHO/User shall provide a verbal explanation of the HMIS database and the terms of consent to the Client, including an explanation of how the information will be used, how it will be provided, and advantages of providing accurate information.
- C.3 The Service Provider/CHO shall maintain appropriate documentation of Client consent to participate in the HMIS database.
- C.4 The Service Provider/CHO/User shall diligently record and take appropriate actions, in the HMIS system, to record all restrictions requested by the Client.
- C.5 If a Client withdraws consent for release of information, the Service Provider/CHO/User remains responsible to ensure that Client's information is restricted.

Privacy Requirements

The Privacy Standards apply to all Covered Homeless Organizations (CHO), Continuum of Care (CoC), Homeless Service Providers, HMIS Users and HMIS host or administrators. All organizations and users that have access to HMIS data must comply with the privacy requirements listed below with respect to; data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. Privacy refers to the safeguarding of Protected Personal Information (PPI) in the HMIS from open view, sharing or inappropriate use.

Covered Homeless Organization (CHO) Responsibilities

A CHO may adopt additional substantive and procedural privacy protections that exceed the requirements listed below as long as all additional protections and procedures are included in its privacy notice. Employees, volunteers, affiliates, contractors and associates are covered by the privacy standards of the CHO they deal with.

- P.1 The CHO must publish a privacy notice describing its policies and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request.
- P.2 The CHO must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures
- P.3 The CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information.
- P.4 The CHO must post a sign stating the availability of its privacy notice to any individual who requests a copy.
- P.5 The CHO must allow an individual to inspect and to have a copy of any PPI about the individual. The CHO must offer to explain any information that the individual does not understand.
- P.6 The CHO must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual, The CHO is not required to remove such information but they may mark such information as inaccurate or incomplete or supplement such information.
- P.7 The CHO must establish a method, such as an internal audit, for regularly reviewing compliance with its privacy notice. The CHO must maintain permanent documentation of all privacy notice amendments
- P.8 The CHO must establish an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of denial of access or correction rights.
- P.9 If the CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page
- P.10 The CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.
- P.11 The CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to undergo (annually or otherwise) formal training in privacy requirements.
- P.12 The CHO must secure any paper or other hard copy containing PPI that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms.

HMIS Use and Responsibilities

HMIS use is the responsibility of all Covered Homeless Organizations (CHO), Users, and the HMIS System Administrator. All CHOs and Users shall abide and comply with all policies and procedures of HMIS and shall keep abreast of all ServicePoint updates and policy changes. Each authorized User is provided an access level within the system as required by his/her role in the CHO and HMIS data entry, and/or reporting (see the User Access Level chart in the Security System section).

Covered Homeless Organizations and their authorized Users shall not misrepresent their client base in the HMIS database by entering known, inaccurate, false or misleading data under any circumstances. The CHO and User will not alter information, with known inaccurate information, that has been entered into the HMIS database by another CHO, Service Provider, Agency, or User.

Covered Homeless Organization and their authorized Users shall not cause in any manner or way known corruption of the HMIS database. **Report any discrepancies in the use of the IHFA HMIS system, including without limitation access of information and entry of information, to the Agency Director or to the HMIS System Administrator.**

The use of the HMIS database with the intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity, will be grounds for legal action.

Covered Homeless Organization (CHO) Responsibilities

- H.1 The CHO who receives HUD funding (SHP, ESG, S+C, etc) participating in HMIS must be current in all related contracts.
- H.2 The CHO shall identify, approve and authorize their respective Users and is responsible for contacting the HMIS System Administrator for revoking, adding or editing User access.
- H.3 The CHO shall be responsible for entering Client data (profile, household, needs, services, referrals, any other Client data you may require), following up on referrals, running reports.
- H.4 The CHO shall provide an email contact to the System Administrator for each User for communication purposes.
- H.5 The CHO shall have representation at all agency/regional data quality review meetings.
- H.6 The CHO shall be responsible for HMIS data entry compliance for client data and reports.
- H.7 The CHO is responsible for the Users data entry accuracy, correctness and completeness. The CHO shall periodically (or when requested by the System Administrator) run and review audit reports to ensure data integrity.
- H.8 The CHO shall designate one User to be the HMIS Key User.
 - The Key User shall use Agency NewsFlash only for the distribution of HMIS information.
 - The Key User shall act as the first level of HMIS support for the CHO
 - The Key User may be responsible for the initial training of new Users for the CHO.
 - The Key User shall regularly review audit reports to ensure staff is following policies.
 - The Key User will be responsible for monitoring all User access within the CHO.

User Responsibilities

- H.9 The User shall only enter individuals in the HMIS database that exist as Clients under the Service Provider's approved area of service.
- H.10 The User shall follow, comply with and enforce the User Agreement. (The User Agreement may be modified, with notification, by IHFA at its discretion, as needed for the purpose of efficient operation of the HMIS system).
- H.11 The User shall be responsible for entering into HMIS:
- HUD funded CHO – Universal Data Elements (client profile, household, entry/exit, services, and shelter), and any Program Specific data as required by the grant.
 - Non-HUD funded CHO – at a minimum the Universal Data Elements (client profile, household, entry/exit, services, and shelter).
- H.12 The User shall consistently enter information into the HMIS database and will strive for weekly data entry. In the event that weekly data entry cannot not be made, the User shall have all data entry completed for the month by no later than the 15th of the following month.
- H.13 If the Users utilized hard copy paper forms to enter data into HMIS, the forms shall be securely stored or suitably disposed of once data entry is complete.
- H.14 The User shall enter ROI information (Client Consent and Release of Information Authorization) on all clients. **Sharing data is optional but entering data is not optional. An ROI shall be recorded for all clients, even if not sharing data.**
- H.15 The User shall not include profanity or offensive language in the HMIS database.
- H.16 The User shall utilize the HMIS database for business purposes only.
- H.17 The User shall follow the Rules for Password and User IDs in the System Security section).

IHFA System Administrator Responsibilities

- H.18 The System Administrator shall provide training and periodic updates to that training to select Service Provider Staff on the use of the HMIS software.
- New, intermediate and advanced User Training
 - Reports Training
 - Program enhancement, upgrades, refresher or other specifically requested training.
- H.19 The System Administrator shall apply patches and upgrades to the system and send out notification and documentations prior to the event.
- H.20 The System Administrator will regularly run review and audit reports. Results of these reports may be shared with Affiliated Service Providers the Continuum of Care, and other organizations as required.
- Draw Audits
 - APR Audits
 - Data Completeness Audits
 - Data Quality or System Security Audits
- H.21 The System Administrator shall provide important news items, updates and alerts via email, newsletters and NewsFlash in ServicePoint.
- H.22 The System Administrator shall be available for technical assistance such as HMIS requirements and procedures, system troubleshooting and report generation.
- H.23 The System Administrator shall aid in the determination of HMIS User access level. The level will be based on each User's job function as it relates to ServicePoint's data entry and retrieval schema (see User Access Levels in the System Security section).

System Security

ServicePoint (Bowman Systems) is a web-based software encrypted for secure transmittal and storage. Implementation of ServicePoint involves a centralized database where participating Agencies, with client consent, can enter and access Client information, and all data is encrypted at the database level. This means that anyone hacking into the server would not see any Client information. This encryption tool is state of the art. All changes, additions and deletions to Client records are tracked by the system and can identify the User and the action. Information can be locked or unlocked, viewed or not, depending on the User Access Level of the viewer. This provides a level of security and accountability for the CHO's database.

Every User of the HMIS system is authenticated with a unique User ID and password. A User will be locked out of the system after four consecutive bad logon attempts and will need to contact the System Administrator to regain access. All Users shall utilize the password protected screen savers on any computer accessing the HMIS database and the User shall log off of HMIS and shut down the browser when not using HMIS.

Covered Homeless Organization (CHO) Responsibilities

- S.1 The CHO must protect the HMIS system from viruses by using commercially available protection software. A CHO must regularly update virus definitions from the software vendor.
- S.2 The CHO must protect the HMIS system from malicious intrusion behind a secure firewall. Each individual workstation does not need it's own firewall, as long as there is a firewall between that workstation and any other systems. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the server through a central server would not need a firewall as long as the server has a firewall
- S.3 The CHO shall ensure that all their authorized Users are issued a unique User ID and password for HMIS and receive confidentiality training on the use of HMIS and applicable confidentiality laws.

Rules for Passwords and User IDs

- S.4 Each User will follow these Rules for Passwords and User IDs:
 - **Sharing of passwords and User IDs is forbidden.** Every authorized User will be issued their own User ID and password. Keep your password secure and confidential.
 - Never use the same password twice. When selecting a new password, choose one that is reasonably different from your previous password.
 - ServicePoint will require a password change every 45 days. Passwords must be a minimum of 8 characters, and include 2 numeric values.
 - Do not select a trivial, predictable or obvious password or a common word found in the dictionary or any of the below spelled backwards.
 - Trivial passwords include common words like 'secret', 'password', or 'computer'
 - Predictable passwords include days of the week, months, or a new password tht has only a one or two character difference from the previous password.
 - Obvious passwords include User name, User ID, names of persons, pets, relatives, cities, addresses, birth date, car license plate and so on.
 - Do NOT use someone else's or password or let anyone use your User ID. If you, or someone at your agency, needs more access, or if you are having problems with your access, contact your System Administrator for help.
 - Beware of "shoulder surfers". These are people who stand behind you and look over your shoulder while you are keying in your password or are working with confidential information.

- NEVER post your login or password on your terminal, under your keyboard or other obvious places.
- Always change the temporary password assigned to you by the System Administrator as soon as you receive it.
- LOG OFF or LOCK UP when you are finished using your terminal or workstation, or if you are stepping away from your desk, even momentarily.
- If you are going to be away from the office for an extended period (e.g. vacation or maternity leave), ask your administrator to temporarily suspend your access. Your ID will be reactivated when you notify the System Administrator or your return.

User Access Levels

The access levels controls who can see which information. Confidentiality is a primary concern and these levels of access help control access to information. Lower levels allow viewing only of basic demographics, while middle levels allow additional information to be viewed, added and/or updated. The highest level allows access to Agency functions and unlimited client access.

Access Level	Description
Resource Specialist I	Access is limited to the ResourcePoint module. This role allows the user to search the database of area agencies and programs and view the detail screens for each agency or program. Access to client or service records is not given. A Resource Specialist cannot modify or delete data.
Agency Staff	Agency staff has access to ResourcePoint, limited access to ClientPoint, full access to service records and access to most functions in ServicePoint. However, Agency Staff can only access basic demographic data on clients (profile screen). All other screens are restricted; including assessments and case plan records. They have full access to service records. Agency Staff can also add news items to the newswire feature. There is no reporting access.
Case Manager	Case Managers have access to all features excluding administrative functions. They have access to all screens within ClientPoint, including the assessments and full access to service records. There is full reporting access with the exception of audit reports.
Agency Administrator	Agency Administrators have access to all features, including agency level administrative functions. This level can add/remove users for his/her agency and edit their agency and program data. They have full reporting access. They cannot access the following administrative functions: Assessment Administration, Picklist Data, Licenses, Shadow Mode, or System Preferences.
System Administrator	The System Administrator has full and complete access to the system.

Reports

Affiliated Service Providers have full reporting access to any clients they serve. There are a variety of canned reports available in ServicePoint along with a Report Writer function which the User has full access. In addition, custom reports may be requested at any time from the System Administrator.

- The CHO, Service Provider and/or User's access to HMIS data on clients it does not serve shall be limited based on the current status of any release of information.
- The general public can request reports for non-identifying aggregate and statistical data by completing a Data Request Form. The HMIS System Administrator will address all requests for data from entities other than Affiliated Service Providers or clients.
- Non-identifying aggregate and statistical data will not contain outliers. Outliers may be removed if they represent less than 5% of any value.

The System Administrator will run system-wide reports to assess the data, quality and level of participation by Affiliated Service Providers. Results of these reports may be shared with Affiliated Service Providers.

Notes