HMIS Security and Privacy Plan

Table of Contents

I. Introduction and Background

This HMIS Security and Privacy Plan (SPP) describes standards for the privacy and security of personal client information collected and stored in the HMIS. The SPP seeks to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. The standards set forth in this SPP are based on principles recognized by information privacy and technology communities.

The SPP provides a framework that mirrors many of the technical standards from the 2004 HUD HMIS Data and Technical Standards, while supplementing that documentation with specific policies that have been developed and implemented throughout the State of Hawai'i, and action steps that all organizations utilizing the HMIS are expected to apply. The SPP outlines baseline standards that will be required by any organization that records, uses, or processes protected personal information (PPI) on homeless clients for an HMIS. The SPP strives to reference procedures that organizations and stakeholders can utilize to enhance the privacy and security of information collected through the HMIS.

Throughout the SPP, baseline standards for evaluating privacy and security requirements will be established. At a minimum, all organizations that record, use, or process PPI on homeless clients must meet these baseline privacy and security requirements. This approach provides a standard level of protection for homeless clients and allows for the possibility of additional protections for organizations with additional needs and resources.

II. Key Terms and Definitions

CoC Program: A program identified by the CoC as part of its service system, whose primary purpose is to meet the specific needs of people who are experiencing a housing crisis.

Continuum of Care (CoC): A collaborative funding and planning approach that helps communities plan for and provide, as necessary, a full range of emergency, transitional, and permanent housing and other service resources to address the various needs of homeless persons. HUD also refers to the group of community stakeholders involved in the decision making processes as the "Continuum of Care."

Contributory HMIS Organization (CHO): An organization that operates a contributory homeless assistance program or homelessness prevention program or contributory non-homeless assistance program.

Coordinated Entry System (CES): The O'ahu Coordinated Entry System (CES) is the O'ahu CoC's approach to coordinated assessment, prioritization and referrals of individuals who are experiencing homelessness or at risk of experiencing homelessness.

End User: An employee, volunteer, affiliate, associate, and any other individual acting on behalf of a CHO or HMIS Lead Agency who uses or enters data into the HMIS or another administrative database from which data are periodically uploaded to the HMIS.

Homeless Management Information System (HMIS): The information system designated by a CoC to process Protected Personal Information (PPI) and other data to create an unduplicated accounting of homelessness within the CoC. An HMIS may provide other functions beyond unduplicated accounting.

HMIS Lead Organization: The organization designated by a CoC to operate the CoC's HMIS on its behalf.

HMIS Administrator: A local administrator established by the HMIS Lead Organization to act as the point of contact for many HMIS related questions. The HMIS administrator also works with numerous stakeholders and CHOs as a conduit for localized HMIS technical assistance.

Homeless Programs Office (HPO): State office housed under the Hawai'i Department of Human Services, responsible for the administration of numerous homeless assistance programs.

Protected Personal Information (PPI): Information about a client: (1) whose identity is apparent from the information or can reasonably be ascertained from the information; or (2) whose identity can, taking into account any methods reasonably likely to be used, be learned by linking the information with other available information or by otherwise manipulating the information.

III. HMIS Privacy Standards

The goal of the HMIS Privacy Standards is to ensure that all required client data will be entered in the HMIS in a manner that maintains the confidentiality and security of the data in conformity with all current regulations related to the client's rights for privacy and data confidentiality.

A. HMIS Privacy Policy and Notice

Policy: All Contributory HMIS Organizations (CHO) that enter data into the HMIS must post the HMIS Privacy Policy and Notice at their workstation or wherever data is collected and entered. The HMIS Privacy Policy describes how information about the client may be used and disclosed, and how the client can obtain access to their information. The HMIS Privacy Notice is a brief document describing a consumer's data rights in relation to the HMIS. Agencies must use the Privacy Policy and Notice attached in the Appendix and must make these available to clients upon request.

This policy may be amended at any time. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

Procedures: Each workstation, desk, or area used for HMIS data collection must post the HMIS Privacy Notice. As Outreach workers gather data in the field, they must have the Privacy Notice available upon request to all clients. This policy will allow Outreach agencies to use an implied consent model, which is outlined in Section D of this Part. If an agency serves non-English-speaking clients, or clients whose primary language is not English, the agency must also provide translation services for the HMIS Privacy Notice. If an agency has a website, the HMIS Privacy Notice must be posted on

that website as well. An agency may also post the HMIS Privacy Notice in a waiting room, an intake line, or any other public area where clients congregate before intake occurs.

B. HMIS Client Consent Form (Release of Information)

Policy: All clients must sign or verbally accept the HMIS client consent form before their PPI can be shared with other agencies in the HMIS. If consent is given verbally, service providers should make reasonable efforts to have a witness present. It is important to note that client information can be entered into the HMIS without consent; however this information cannot be shared with other organizations unless written or verbal consent is received. All HMIS client consent forms must be stored securely for a minimum of seven years after the client last received services from the agency and uploaded in HMIS. Agencies must give a copy of the consent form to clients if requested. PIC's current HMIS client consent form is documented in the Appendix.

Procedures: Each adult client must sign or provide verbal acceptance of the HMIS client consent form before their information and information of their dependents may be shared with other agencies in the HMIS. If consent is given verbally, service providers should make reasonable efforts to have a witness present to sign the consent form in the indicated place. The HMIS client consent form is valid for three years from the date of signature whereby the client consents to share their data. PPI collected before expiration may still be used in perpetuity after expiration of the consent unless a client files a form to redact the original consent. It is important to keep the consent form on file for auditing purposes for at least seven years. Consent forms must be kept securely in accordance with standard confidentiality and privacy practices (e.g. locked in a file cabinet and not accessible without authorization).

It is recommended that agencies keep the consent form with the established client file along with other information that is being collected and maintained. Agencies may also wish to voluntarily give all clients copies of their signed client consent form.

C. Offsite Data Entry

Policy: Outreach providers and other HMIS users can collect client-level data in many different settings, including the street, places not meant for human habitation, and homeless service providers' facilities. Because these locations are not ideal for data entry, outreach providers must not enter client-level data into the HMIS through tablets or other wireless devices via an unsecured wireless network unless there is end-to-end encryption from device to website/application programming interface (API).

Procedures: Outreach providers and other HMIS users must ensure that the internet connections used to access the HMIS from their facilities are set up using basic standard network security protocols to prevent unauthorized access to the network and to HMIS data stored in local servers or hard drives.

Because of the confidential nature of data stored within HMIS, the system must be accessed from a sufficiently private physical location to ensure that persons who are not authorized users of the HMIS are not able to view client-level data.

Because these standards are important for the protection of client-level data, outreach providers and other HMIS users must not enter client-level data over unsecured public wireless internet connections. If secure wireless connections are not available, outreach providers and other HMIS Users should gather information on paper for data entry at a later time when a proper internet connection can be accessed.

D. Presumed Client Competence

Policy: All organizations should presume that all clients are competent unless a currently effective court order finding incompetence is known. If an end user determines a client is not competent to consent for any reason, the end user will seek guidance from a program manager or the HMIS administrator.

Procedures: Industry wide best practice is to presume that all clients are competent unless there is a known court order stating otherwise. If there is a known court order stating the individual is not competent, then it will not be possible to obtain client consent for the HMIS. In this case, CHO end users may enter client information into the HMIS, but that information must not be shared with other CHOs. If there is no court order, CHO end users should do their best in attempting to obtain consent to share from individuals that may not appear to be fully competent during intake. Participants who are under 18 years of age must gain verbal or signed consent from a parent or guardian.

E. Denial of Services

Policy: Clients do not have to participate in the HMIS to receive program services. Agencies cannot deny services to an individual solely on the basis of the individual deciding not to participate in HMIS. Some clients will choose not to share data in the HMIS or will not be capable of making an informed consent; however, it is important that these clients are not prohibited from receiving services by the program.

Procedures: If a client decides not to share their data in the HMIS, an agency cannot deny services because of that decision. Agencies are not required to guarantee services to an individual. Individuals may fail to meet eligibility criteria, there is a lack of openings, and/or there is a lack of funding. Agencies may determine if an individual will or will not receive services before the individual goes through the informed consent process. This will eliminate a perceived relationship between HMIS participation and service delivery.

F. User Authentication

Policy: Each end user must fill out an HMIS user agreement form. Additionally, when HMIS end users leave or are terminated from the organization, agency administrators must notify the PIC HMIS Administration team at hmis@partnersincareoahu.org within 24 hours so that the end user can be removed from the HMIS. All users with no login activity for at least three months will be automatically deactivated.

Procedures: Each end user and their Agency's Authorized Point of Contact must sign a user agreement before the end user may gain access to the HMIS. A copy of the current PIC HMIS user agreement is located in the Appendix. The Authorized Point of Contact must email the completed form to hmis@partnersincareoahu.org. End users and their CHO are ultimately responsible for all actions occurring in the system under their login information. Auditing and access log functionalities are part of the HMIS, which implies that specific user tasks and procedures can be traced.

The HMIS Administration team must be apprised within 24 hours when HMIS end users exit employment voluntarily, are terminated, or are laid off so these users' accounts can be deactivated. CHOs repeatedly failing to adhere to this policy may see funding adversely affected.

The HMIS Administration Team will deactivate the accounts of any users who have not logged in for three months. To reactivate an account, the Agency's Authorized Point of Contact must email to hmis@partnersincareoahu.org to request reactivation. The HMIS Administration Team will require re-training on a case-by-case basis.

G. HMIS Data Sharing

Policy: HMIS client data cannot be shared with other organizations unless explicitly authorized by the client through the client consent form in the Appendix. Currently, all organizations have the potential to share data except Run away and Homeless Youth providers, who can only share data in certain circumstances (RHY programs whose participants are over 18 years of age must sign a consent form or indicate verbal acceptance of the consent form. HIV/AIDS, mental health, and substance use providers can share data with appropriate informed consent. Data sharing must be manually selected for each client in order for it to take effect.

Procedures: The HMIS is capable of sharing client historical data, which includes services and basic demographic data including but not limited to: name, age, gender, race, ethnicity, family members, marital status, history of domestic violence, housing history, disabling conditions, VI-SPDAT survey data, SPDAT survey data, program intake dates, encounter dates, program discharge dates, employment status, income and non-cash benefits, health insurance, case notes, eligibility documents, and housing plan. It should be noted that a client's SSN and DOB can be seen as part of the search.

CHO users will keep client data confidential at all times and will obtain client consent to share client PPI via the HMIS. The HMIS application allows agencies to share service records, which allows them to coordinate services more efficiently. Part of the CoC monitoring policy will be to ensure that client's electing to share data on paper were also selected to share data via the HMIS. This policy aligns with Section B above.

HMIS is utilized to support coordination of services, report data and outcomes for funders of services and ensure programs are compliant through monitoring and evaluation. HMIS is not used to track people experiencing homelessness for political reasons and/or for perpetuating the criminalization of homelessness. The Data Committee and CoC Advisory Board will review requests for HMIS access from active paid members of the CoC, and will not approve requests that are inconsistent with HMIS' purposes. Aggregate data may be requested and entities collaborating with agencies who utilize HMIS is encouraged but no client level data will be disclosed.

H. Client Access to Their Records

Policy: Clients have the right to receive a copy of their data that exists in the HMIS. This policy must be present in the HMIS Privacy Notice and is outlined in item A of this section. Agencies must be able to accommodate this item but are advised not to make copies for clients unless it is requested. Client's may lose or misplace PPI via paper forms, which may increase the likelihood of the information being used for malicious purposes.

Procedures: Clients may request a copy of their information contained within the HMIS. Agencies are required to provide them with a copy of the universal and program specific information if it is requested and if the client has identification documents proving they are the client of record. Agencies are not required to print out any additional information, although it is optional and allowed.

I. Client Grievance Process

Policy: Clients have the right to file a grievance with the CHO concerning violations of their privacy rights regarding their HMIS participation. No action or punishment may be taken against a client if they choose to file a grievance. The grievance form is found in the Appendix.

Procedures: A client must request and complete the CoC's standard grievance form. The client may turn the form into an organization not related to the grievance or may mail the form to the CoC.

The CoC will review the grievance, research the nature of the complaint, and will respond to the grievant within 30 days. The agency named in the grievance, the CoC, and other participating HMIS agencies will not refuse or reduce services to the client because of a filed grievance. A thorough investigation by the CoC will ensue if a client reports retaliation due to the filed grievance.

J. Research Agreements

Policy: Research agreements between organizations may be enacted for the purposes of analysis and distribution of HMIS data. This research may be conducted so long as agreements are drafted between organizations before data is supplied or received. Conclusions and analysis must be presented in the aggregate and must not display any client PPI.

Procedures: Formal agreements must be established between organizations before HMIS data is supplied. An example of a formal research agreement that can be used is presented in the Appendix of this Plan. Agencies may revise the agreement as needed. To submit a data request or research agreement to the Data Committee for review, complete the document found in the appendix and submit it to hmis@partnersincareoahu.org.

K. Data Integration Requests

Policy: Agencies who enter data into another instance of the HMIS for internal use may request to integrate their data into HMIS to eliminate the need for double data entry. The cost for the data integration will be assumed by the requesting agency. Requests for integration will only be considered if the agency utilizes the same vendor as the CoC. The software solution provider will determine the frequency of data integration and the data integration flow (one-way or two-way, real-time or batched).

Procedures: All data integration requests are to be sent to the PIC Data Committee Chair for consideration at the next PIC Data Committee Meeting.

- Describe how the data quality and data improvement process will work without involvement of the HMIS Lead or HMIS System Administration

The Data Committee will make a recommendation on the data integration request with a simple majority vote of a quorum from the Data Committee voting members. If the Data Committee recommends data integration, the approved data integration request will be sent to the requesting Organization. If the Data Committee does not recommend data integration, the Organization will be notified via e-mail by the Data Committee Chair and will be offered a rationale for the decision to deny the data integration request.

IV. HMIS Security Standards

The goal of the HMIS Security Standards is to ensure that HMIS data are collected, used, and maintained in a confidential and secure environment at all times. The HMIS Security Standards applies to the Partners in Care, CHOs, and the overall HMIS software vendor. Specific applicability is described in each policy within these security standards. These standards apply to all PPI collected in the HMIS or uploaded through comparable databases.

Partners in Care recognizes that agencies may have established their own security policies that meet the HUD security requirements and minimum standards set forth below. The purpose of this document is to outline those standards to all CHOs and define the parameters of compliance with these standards. This document is not intended to supplant individual CHO security policies, but rather to supplement them. As long as CHO policies and practices meet the minimum thresholds established in this plan, they may establish additional or more stringent security requirements. Another key purpose of this document is to describe how Partners in Care will meet and maintain security requirements established in HUD's security standards.

A. Password Privacy Requirements

Policy: Each end user must have distinct login information that is not shared. It is imperative that end users never share their login information with anyone, including coworkers or managers.

Procedures: End users receiving access for the first time will be assigned a default password. Upon first login, users will be prompted to change their password. User Passwords should be at least eight characters long and include the following:

- At least one number and one letter
- Not using the username, the HMIS name, or the HMIS vendor's name
- Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

If someone is having trouble accessing the HMIS or has been locked out of the system, they should utilize the software provider's 'Forgot my password' feature on the login screen to reset their account. Further difficulties should be escalated to the PIC HMIS administration team at hmis@partnersincareoahu.org.

Users will be prompted to change their password every three months.

Sharing login information with another person is a direct violation of the HMIS user agreement and this Plan. An end user's username and password must not be stored or displayed in any publicly accessible location. Sharing username and password is strictly prohibited. Users violating this will be subject to penalties detailed in the Security and Incident Procedures section of this document.

B. Levels of User Access and Security

Policy: Each CHO will maintain a written policy detailing organizational management control over access authorization, user levels, and the internal process for activating new HMIS users. The Data Committee will be solely responsible for authorizing new agency access to the HMIS, and the HMIS Administration team will be solely responsible for establishing new users in the HMIS. The highest HMIS access level of system administrator will only be assigned to members of the HMIS Lead Organization.

Procedures: CHOs must establish an internal point of contact (POC) who will be the conduit for establishing new users with the HMIS administration team. Individual staff should not email the HMIS administration team to request new HMIS users or expanded access to HMIS. This is important from a security standpoint, as staff may no longer be employed with the organization.

The Oahu HMIS has the following user types:

- Authenticated Users –This user type is able to view and edit client data. Service providers are assigned this user type.

- Alter Own Role –Only the PIC HMIS Administration team has access to Alter Own Role. These users are able to alter the role (Case Management, VI-SPDAT, Agency Admin, etc.) they have been assigned.

- Alter Any Role – Only the PIC HMIS Administration team has access to the Alter Any Role. These users are able to change all roles and workflows.

C. Security Incident Procedures

Policy: Security incident procedures elicit a two-tiered approach:

- A user who breaches the terms of the HMIS user agreement will face sanctions specified by the CoC so that repercussions are uniform and fair for all CHOs. These specifications are required to be documented as part of the HMIS security plan. Any breaches related to security or privacy must be reported to the HMIS Lead within three business days of discovery. These breaches will be dealt with on a case-by-case basis by the HMIS Lead. The CHO assumes all responsibility for negligence due to data breaches or risk of incident within the organization.

- All HMIS users are obligated to report suspected instances of noncompliance with these Standards that may leave HMIS vulnerable to intrusion or compromise client PPI. Partners in Care and HMIS Administration team are responsible for reporting any security incidents involving the real or potential intrusion of the HMIS to the CoC. Each CHO is responsible for reporting any security incidents involving the real or potential intrusion of the HMIS to the HMIS Lead Organization.

Procedures: Associated measures for dealing with suspected policy violations or actual breaches of the HMIS in accordance with the above policies are outlined below.

At minimum, a letter documenting the violation and involved personnel will be sent to the HMIS participating agency from Partners in Care. A copy of the letter will stay on file with the PIC HMIS Administration Team. The HMIS Participating Agency must submit to the HMIS Lead Organization a written plan for corrective action, including any internal actions taken against employee(s) who violated policy. This must be received within 10 business days, and corrective action must be taken within 30 days.

Other penalties may include, but are not limited to:

- Mandatory retraining to be attended by the offending user, the Authorized Point of Contact, and other agency staff identified by the HMIS Lead Organization or the HMIS participating agency,
- A temporary or permanent ban from using the HMIS,
- Onsite security audit using Security and Privacy Plan Checklist,
- Loss of agency access to HMIS, and

- Legal action

The HMIS Lead Organization has implemented these baseline written policies for managing a breach of the HMIS user agreement. The CHO Authorized Point of Contact should use all reasonable measures to ensure staff comply with these policies. At minimum, CHOs will inform users that unauthorized use or disclosure of PPI is considered a serious matter and will result in penalties or sanctions, which may include:

- The loss of use or limited use of the HMIS and other office and technology resources;
- Financial liability for any costs that may arise through user negligence;
- Adverse employment actions including dismissal;
- Civil and/or criminal prosecution and penalties

At site monitoring, each CHO will indicate in the Security Certification Checklist whether or not such a policy exists. If such a policy does not exist, the CHO must develop and implement such a policy within three months of the date of the site monitoring. The CHO must provide the HMIS Lead Organization with the policy.

HMIS users will report any incident in which unauthorized use or disclosure of PPI has occurred. CHO users will report any incident in which PPI may have been used in a manner inconsistent with the HMIS Privacy or Security Standards. Security breaches that have the possibility to impact the Oahu HMIS must be reported to the Authorized Point of Contact and the HMIS Lead Organization. Each CHO will maintain and follow CoC-wide procedures related to thresholds for security incident reporting.

The CoC and HMIS Lead Organization staff, in conjunction with the CoC, will review violations and recommend corrective and disciplinary actions. Each CHO will maintain and follow procedures related to internal reporting of security incidents.

D. Audit and Access Controls

Policy: The HMIS will maintain an accessible audit trail that allows the monitoring of user activity.

Procedures: The HMIS Administration Team will use the software vendor's audit functionality in situations of misusage of HMIS by end users. End users will be subject to the penalties listed in "Security Incident Procedures."

E. Personnel Clearance.

Policy: To the extent possible, a background check should be initiated for all users prior to the provision of HMIS access. If a background check is completed, any user with history of crimes related to identity theft or fraud must not be allowed access to the HMIS.

Procedures: Organizational policy should mandate the denial of access to personnel that have criminal history relating to identity theft or fraud.

F. Malware and Virus Protection with Auto Update

Policy: All CHOs accessing the HMIS must protect the system by using commercially available malware and virus protection software. CHOs must also protect the workstations accessing the HMIS from malicious intrusion by maintaining a secure firewall.

Procedures: Virus and malware protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is accessed. A CHO must regularly update virus definitions from the software vendor. There must be a firewall between the workstation and any systems, including the Internet and other computer networks, located outside of the organization.

G. Workstation Privacy

Policy: In an effort to keep the HMIS and client data secure, end users and CHOs must implement the following security measures.

- End users' computer screens should be placed in a manner where it is difficult for others in the room to see the contents of the screen. Workstations should not be in common areas where clients or other non-HMIS staff can gain access.
- End users should not write down usernames and passwords and store them in an unsecured manner. This includes posting password and/or login information visibly near the workstation.
- When end users are away from the computer, they should log out of the HMIS or lock down their workstation.
- Computers used for HMIS data entry or analysis must have locking screensavers with password protection. Screensavers should lock after five minutes of inactivity

Procedures: The following procedures correspond with the above policy requirements and are mandatory for all CHOs.

- Monitor placement plays a role in establishing security within an organization. End users should consider placing the monitor in a manner so that it is difficult for others to see the screen. This will help to protect the privacy of client PPI.
- Never post HMIS login and password information under your keyboard, on your monitor, or out in the open. Implementation of this policy will make it difficult for others to obtain your login information and access into the HMIS.
- End users stepping away from their computers must log completely out of the HMIS. Locking down the workstation is also a good policy if PPI is stored locally.
- CHO IT departments must implement locking screen savers on all computers used for HMIS data entry or analysis.

H. Disaster Protection and Recovery

Policy: The HMIS Vendor must have a plan for maintaining and recovering access to HMIS data in the event of disaster.

Procedures: The HMIS Vendor will include provisions to maintain a backup of the HMIS data at a separate physical location consistent with the most up-to-date HUD HMIS security standards. The HMIS hosting entity will back up all HMIS data daily. All backups will be held securely at a secondary data center within the hosting entity. To the extent possible, all data will be copied to a second server so that if an entire server malfunctions, data will be available immediately with no service interruption. The failover function will be tested at least once per year and after each major system upgrade.

I. Hardware/Software Management & Physical Safeguards

Policy: The HMIS Vendor will ensure that the hosting entity maintains protections for the physical security of the facilities and media in which HMIS data is stored.

Procedures: The HMIS Vendor will use a secure public cloud computing platform used for analytics, storage and networking. If the Vendor is using an onsite server environment, physical safeguards within the hosting entity include secure site storage, power grids, uninterrupted power supplies, air conditioning, and disaster prevention and recovery systems. The HMIS Vendor will utilize multiple hard drives and redundant power supplies to minimize interruption to service. At a minimum, the HMIS data will be stored in a facility with appropriate temperature control and fire suppression systems. Surge suppressors must be used to protect systems used for collecting and storing all HMIS data.

J. Wireless Transmission Security

Policy: The HMIS Vendor is responsible for ensuring that HMIS Secure Sockets Layer (SSL) certificates are kept current. CHOs will specify in their security standards that sensitive PPI such as SSNs will not be transmitted over the internet through email accounts. Policies regarding the transmittal of HMIS username and password information must be established and assert that each piece of login information must not be sent in the same email. Users accessing the HMIS outside of the workplace are held to all standards within this Plan and assume all risks associated with potential breach of HMIS data.

Procedures: SSL (Secure Sockets Layer) is standard security technology for establishing an encrypted link between a website and a browser. SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. The SSL protocol determines variables of the encryption for both the link and the data being transmitted. It is the responsibility of the HMIS Vendor to retain a current certificate.

Each CHO must establish policies within its security plan so that PPI is not transmitted over the internet via email unless the email is encrypted. Username, password, and HMIS URL information

must not be sent in the same email as a defense against potential threats to the HMIS. Users accessing the HMIS on their personal computer without using a protected shared server are expected to adhere to the same policies as outlined in this Plan.

H.R.S. § 487N-1 et seq. applies to non-encrypted electronic personal information under a definition which includes PPI. Unauthorized disclosure of PPI by a CHO can trigger regulatory investigations. Every CHO is therefore responsible for abiding by Hawai'i revised statutes that include electronic transfer of PPI.

K. CHO Data Safeguards Outside of HMIS

Policy: Any CHO that downloads client-level data from the HMIS will take full responsibility for safeguarding the data with the same security and privacy protocols as outlined in the HMIS Policies and Procedures. This policy is for HMIS client records as well as any reports where client-level information is included, such as a By Name List.

Procedure: Any client-level data downloaded from the HMIS must be encrypted via password-protection immediately. Any client-level data printed must be stored in a locked file cabinet or shredded when it is not being used. CHO or HMIS users assigned to a CHO will be held responsible should client-level data be removed from HMIS and not protected to the standards set forth in the HMIS Policies and Procedures. The most likely source and risk for a client-level data breach is data downloaded from the HMIS and managed improperly at the CHO-level. Each agency will have an annual review (See the appendix for the Security Certification Checklist) by the CHO designated Agency Administrator that affirms any data removed from HMIS is protected to the standards laid out in the HMIS Policies and Procedures. Failure to follow this process could lead to the CHO losing access to the HMIS.

V. MONITORING

It is the responsibility of the CoC, the HMIS Lead Organization, HMIS Participating Organization Executive Directors, and all service providers conduct monitoring and provide notification to the CoC of the progress of participating programs.

It is the responsibility of HMIS Participating Organizations to comply with the HMIS Data Quality Plan and to collaborate with the HMIS Lead Organization and support staff to quickly correct data that does not meet the compliance thresholds.

Policy
The HMIS Lead Organization and support staff will conduct annual on-site monitoring using the Privacy and Security Certification Checklist found in the Appendix. HMIS Participating Organizations should continuously self-monitor using this same Checklist. Agencies determined to be 'Not Meeting' the requirements of the Privacy and Security Certification Checklist will work with the HMIS Lead Organization and support staff to determine a date by which the elements will be

implemented. The Data Committee and HMIS Lead Organization, in conjunction with the rest of the CoC, will review violations and recommend corrective and disciplinary actions.

Procedure

The HMIS Lead Organization will work with the HMIS Participating Agency's Authorized Point of Contact to schedule an on-site monitoring appointment. Partners in Care staff will arrive at the agency with the Privacy and Security Certification Checklist in the Appendix. The Authorized Point(s) of Contact and the HMIS Lead Organization staff will determine if the HMIS Participating Agency meets or does not meet each requirement.

If the HMIS Participating Agency does not meet the requirement, a date will be set for the Participating Agency to come into compliance. A maximum of 1 month is allowed for the Agency to make the necessary changes. Any agencies not meeting all required elements within 3 months will be subject to the penalties listed in this security and privacy plan. The penalties will be determined by the CoC.

APPENDIX

A. Client Consent Form

B. Agency Participation Agreement

C. Grievance Form

D. Formal Research Agreement

E. Data Request or Research Agreement

F. Privacy and Security Certification Checklist

G. Privacy Notice