Philadelphia Homeless Management Information System (PA HMIS)

Appendix A: PRIVACY AND SECURITY PLAN

Contents

DEFINITIONS

Covered Homeless Organization (CHO)

Any organization (employees, volunteers, and contractors) that records, uses or processes

Protected Personal Information Protected Personal Information (PPI)

Any information about a homeless client that (1) identifies a specific individual, (2) can be manipulated so that identification is possible, (3) can be linked with other available information to identify a specific individual

ARTICLE 1: PURPOSE

This document describes the privacy plan of the City of Philadelphia Office of Homeless Services (OHS), which is the Philadelphia Continuum of Care HMIS Lead Agency, and agencies contributing data (HMIS Participating Agencies (HPA)) to the Philadelphia Continuum of Care Homeless Management Information System (HMIS). This document covers the processing of Personal Identifying Information (PII) for clients of HMIS Participating Agencies.

Clients are uniquely identified by a database-managed identity field. For reporting purposes, HMIS usually de-duplicates clients at the Program level, per HUD-accepted practice. For purposes of system-wide data sharing and de-duplication, clients with a high enough threshold of quality profile data are identified by a globally unique Master Client ID, which allows system-wide de-duplication. These global IDs are constantly maintained by the system with algorithms that examine client data to determine if matches can be made as data is updated/ added.

ARTICLE 2: ROLES AND RESPONSIBILITIES

System Administrator

Full privileges to HMIS - HMIS System Administrator, Help Desk, and programmers only.

HMIS Lead

A rarely used "super user" privilege level used by OHS staff to allow "Manage Agency" access to multiple agencies (a service area). In jurisdictions that have an HMIS lead, certain System Administration duties, such as enforcement of policies and procedures may be assumed by this individual on behalf of the System Administrator.

Responsibilities of HMIS Lead Agency

As HUD mandates, the HMIS Lead Agency shall:

1. Establish a security plan;
2. Designate a security officer

a. Criminal background check must be conducted on the designee and other users with administrative privileges;
3. Conduct workforce security screening;
4. Report security incidents;
5. Establish a disaster recovery plan;
6. Conduct an annual security review;

CoC HMIS System Administrator / Agency Manager

The Agency Manager is authorized by their agency's Executive Director within the agency having the appropriate authority. The Agency Manager cannot use HMIS until after signing a HMIS User Agreement with their agency, and completing the required trainings. The Agency Manager is responsible for following the policies and procedures outlined in this document, and are ultimately responsible for collecting and entering client data in as real time as possible depending on the project type. The Agency Manager will also act as the point of contact for client data and reporting done within the system.

Agency Managers are responsible for the following:

1. Designates a security officer
   a. Criminal background check must be conducted on the designee and other users with administrative privileges;
2. Conducts workforce security measures;
3. Ensure that each user completes security training at least annually;
4. Conducts an annual security review;
5. Serves as the primary contact between the Authorized Agency and OHS.
6. Must have a valid email address and be an active, trained user.
7. Manages agency user accounts; adding and removing authorized users for their agency; Agency Managers are required to remove users from the HMIS immediately upon termination from agency, placement on disciplinary probation, or upon any change in duties not necessitating access to HMIS information. All changes must be relayed to the HMIS System Administrator or proxy.
8. Must be technically proficient with web-based software since he/she will be responsible for maintaining the Authorized Agency's HMIS organizational structure and information.
9. Has access to all client data, user data, and agency administration information for the Authorized Agency; thus, is responsible for the quality and accuracy of this data.
10. Ensures the stability of the agency connection to the Internet and HMIS, either directly or in communication with other technical professionals.

11. Trains agency end users, if necessary; this includes training all Authorized Agency staff on how to use HMIS as well as training to ensure compliance with privacy and security policies.
12. Provides support for the generation of agency reports.
13. Monitors and enforces compliance with standards of client confidentiality and ethical data collection, entry, and retrieval at the agency level.

Case Manager

The Case Manager is authorized by their agency's Executive Director within the agency having the appropriate authority. TheCase Manager cannot use HMIS until after signing a User Agreement with their agency, and completing the necessary training. The Assistant Agency Manager / Case Manager is responsible for following the policies and procedures outlined in this document, and are ultimately responsible for collecting and entering client data in as real time as possible depending on the project type.

Clients

Clients choose to participate in HMIS with written authorization to allow an agency's user to collect and enter their personal information into HMIS. It is extremely important in the use of that client confidentiality, privacy, and security are maintained at a very high level. The policies and procedures written in this document fulfill basic HUD HMIS requirements, utilize best practices for the industry, and are further enhanced for the Balance of State CoCs.

ARTICLE 3: HMIS SECURITY PLAN

User Authentication

Upon successful completion of training and subject to approval by OHS, each HMIS user will be provided with a unique personal User Identification Code (User ID) and initial password to access the HMIS.

While the User ID provided will not change, HUD standards require that the initial password only be valid for the user's first access to the HMIS. Upon access with the initial password, the user will see a screen that will prompt the user to change the initial password to a personal password created by the user.

A. Only the user will know the personal password he or she creates. It is the user's responsibility to remember the password.

B. The password created by the user must meet the following Federal and application-enforced guidelines:

- The password must be at least eight characters long.
- The password must contain at least one letter (A through Z and/or a through z).
- The first character of the password must be a letter (A through Z or a through z).

- The password must contain at least one number (0 through 9).
- The password must contain at least one symbol or punctuation character (i.e. $, #).
- The password may not contain your User ID.
- The password may not contain the consecutive upper- or lower-case letters "HMIS" or "hmis."

Providers are responsible for communicating all staff departures to the HMIS Helpdesk in a timely manner to ensure user profiles for departed staff are inactivated.

C. The password may not be stored in a publicly accessible location and written information pertaining to the User ID, password, or how to access the HMIS may not be displayed in any publicly accessible location.

D. The user is not permitted to divulge this password or to share this password with anyone.

E. User permissions are assigned by role and by Agency/Site

F. Users are logged out of the system after a configurable period of inactivity (15 minutes)

G. Passwords must be changed periodically (90 days)

H. Inactive users can be locked out, if necessary

An audit trail of changes is maintained for all user-editable objects in history tables that track when changes were made, by whom, and the previous value(s).

HMIS uses HTTPS/SSL Standards for data transmission.

Password expiration is handled by HMIS Helpdesk. The password rules are: Passwords must be at least six (8) characters long and contain at least one upper-case letter, one lower-case letter, one number, and one symbol. Passwords must be updated every 90 days, and cannot be reused.

Baseline Requirements

A CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes and servers.

Security has three categories:

- System Security
- Software Application Security
- Hard Copy Security

Additional Requirements

A CHO may commit itself to additional security protections consistent with HMIS requirements by applying system security provisions to all electronic and hard copy information that is not collected specifically for the HMIS. A CHO may also seek an outside organization to perform an internal security audit and certify system security.

System Security: User Administration

Authorizing Personnel for HMIS

Policy: *Only authorized individuals who have successfully completed the requirements for access to the system including training and completion of a System User Agreement may be allowed to access HMIS on behalf of an agency.*

HMIS User License Agreement

Policy: *A HMIS System User Agreement must be signed and kept on file for all agency personnel or volunteers, past or present that will collect or use HMIS data on behalf of the agency. The original signed HMIS System User Agreement will be filed at OHS in the agency's HMIS file. Additionally, each agency is required to keep a copy of all of their HMIS System User Agreements on file at their office location so that OHS may review this documentation during monitoring visits. At No Exceptions should an individual who has not signed a HMIS System User Agreement be able to have or gain access to use of a HMIS System User License at any time.*

Description:

The HMIS System Agreement is a document between a participating agency and its employees, contractors, or volunteers who are authorized to collect HMIS data and/or record client data into the system, for the purpose of agreeing to abide by the rules and regulations defined in the HMIS Data and Technical Standards, Final Notice, Federal Register, Volume 69, No. 146 as published on Friday, July 30, 2004.

Designate Agency System User

Policy: *The agency's Executive Director or an Agency designated personnel must designate individuals to act as the agency's System User(s).*

Description:

The System User is accountable for the following items:

- Maintain the agency programs and services profiles in the system;
- Act as the main point of contact for HMIS System Administrator on behalf of their Agency;
- Ensure client privacy, confidentiality, and security;
- Maintain compliance with technical requirements for participation;
- Store and enforce System User Agreements;
- Post Compliance Notice;
- Enforce data collection, entry, and quality standards in a real-time process
- Assist OHS with On-Site Technical Assistance/Audits

Designating HMIS System User License

Policy: *Any individual working on behalf of the agency (employee, contractor, and volunteer), that will enter information into the HMIS database must be designated as a HMIS System User; and therefore is subject to these policies and procedures.*

Description:

Anybody who collects any HMIS data (electronic or paper) or creates reports from the system must receive training. This training is varied depending on the person's role. If someone will not be entering anything into the system but will be explaining HMIS to others, the System Agency Manager is required to train this person on client privacy, confidentiality, and security procedures. Individuals, who will work with the HMIS software, will be required to attend the Policies and Procedures training as well as specific training on the HMIS software.

Assigning User Workgroup Permissions Level

Policy: *The HMIS System Administrator will assign users an appropriate User Workgroup Permissions level such that the users only has access to HMIS functionality or information required to successfully fulfill their agencies roles. The HMIS System Administrator will also maintain the agency's Approved Users List. The Executive Director or empowered officer will then contact HMIS System Administrator to set-up user Workgroup Permissions Levels in the system and to schedule their designated HMIS System User(s) for training. User ids and*

passwords will not be distributed to new users until after they have completed the required HMIS trainings for the HMIS Implementation.

Description:

Within HMIS, each user is assigned a workgroup permission level based on the tabs to which they have access. This security allows the user to gain access to certain areas of the HMIS application. This security feature is utilized to ensure that individuals can only access the type of client information they need to do their job within the agency. An example would be that an agency would be assigned two different workgroup permissions. Agency Manager is designated for the entire agency and can view all information for all programs within their agency only. Case Manager is designated for the individual program within the agency, therefore would only have access to view information for the individual program within the agency.

User Workgroup Permission Levels

Policy: *All HMIS Users will have a level of permission to data that is appropriate to the duties of their position so that information is recorded and accessed on a "need to know" basis. All users should have the level of access that allows efficient job performance without compromising the security of the HMIS or the integrity of client information.*

Procedure: Each Agency Manager (and/or its Executive Director) will identify the level of access each licensed user will have to the HMIS database. Privilege levels were detailed previously in the roles and responsibilities section.

Removing Authorized Personnel

Policy: *The HMIS System Administrator must be notified within 24 hours and in writing by the designated Agency personnel when an individual is no longer authorized to access HMIS on the agency's behalf.*

Passwords

Policy: *Users will have access to the HMIS via a user name and password. Passwords must be changed a minimum of once every 90 days. Users will keep passwords confidential. Under no circumstances shall a user share a password nor shall they post their password in an unsecured location; to do so will be considered a breach of the system user agreement and will trigger appropriate repercussions and/or sanctions for both the user and agency.*

Procedure: *Upon sign in with the user name and temporary password, the user will be required by the software to select a unique password that will be known*

only to him/her. Every 90 days, passwords are reset automatically by the HMIS software. User has a maximum of up to seven times to enter the correct login information. After seven (7) times of failed logins the system automatically locks out the user account for security purposes and the password will have to be recovered/ reset.

Password Recovery

Policy: *HMIS staff has access to User accounts, but not unique passwords. Users must contact the HMIS Helpdesk for password resets.*

Procedure: In the event of a lost or forgotten password, the user will have to send a HMIS Helpdesk ticket to reset their password. Within the helpdesk request the following should be included; username, organization, and that the password needs to be reset. Once users receive an email back from the HMIS Helpdesk, which contains a temporary password, Users must login and change their password immediately before HMIS will allow them access to Agency and Client data.

OHS Communication with Authorized Agencies

Policy: *The HMIS System Administrator or proxy is responsible for relevant and timely communication with each agency regarding the HMIS. The HMIS System Administrator or proxy will communicate system-wide changes and other relevant information to Agencies as needed. He/she will also maintain a high level of availability to Authorized Agencies.*

Procedure: General communications from the HMIS System Administrator will be directed towards all users. Specific communications will be addressed to the person or people involved. The HMIS System Administrator will be available via email, phone, and mail. The notification function in HMIS and the HMIS email list will also be used to distribute HMIS information. While specific problem resolution may take longer, the HMIS System Administrator will strive to respond to Authorized Agency questions and issues within 24 hours of receipt. Agency Managers are responsible for distributing information to any additional people at their agency who may need to receive it, including, but not limited to, Executive Directors, client intake workers, and data entry staff. Agency Managers are responsible for communication with all of their agency's users.

Authorized Agency Communications with OHS (non-technical, i.e. Policy and System Administration)

Policy: *Authorized Agencies are responsible for communicating non-technical needs and questions regarding the HMIS directly to the HMIS System Administrator. In order to*

foster clarity both for HMIS users and for HMIS, ALL non-technical communications with OHS regarding the HMIS must go through the HMIS System Administrator.

Procedure: Agency Managers at Authorized Agencies will communicate needs above and beyond daily help desk technical assistance needs directly with the HMIS System Administrator. Examples of these needs are, but not limited to questions about policies, administration, data requests, and system changes. The HMIS System Administrator will attempt to respond to Authorized Agency needs within two business days of the first contact.

Backup procedures, off-site storage facilities and locations where the backup is stored

ClientTrack Hosting & Backup

ClientTrack's data center is a SSAE 16 certified data center. Incremental database backups are performed every 3 hours and full database backups are performed each day and sent offsite weekly to a second geographically disperse SSAE 16 storage facility.

A. Restoration procedures for the application and data at the host level.
B. Recovery procedures for historical data at the host level.
C. A stated recovery time after a planned or unplanned outage, power interruption, or system crash.

ClientTrack Restoration and Recovery

ClientTrack partners with ViaWest, a state of the art managed hosting and colocation datacenter. ViaWest is an SSAE 16 (formerly SAS 70) certified and co-located data center. Data backup and server recovery are covered as part of standard ClientTrack contracts. HMIS data is backed up on regular intervals throughout the day and daily backups are maintained for approximately 30 days. Backups are stored on spinning disks so there is limited hardware (old tapes) that need destroyed in accordance with HIPAA guidelines upon decommissioning. Failed drives are properly decommissioned to ensure compliance. Data backup is performed to ensure that hardware and drive failures do not result in the loss of data or system availability. Hosting services include:

- Incremental database backups are performed every 3 hours
- Backups are encrypted with 256-bit AES encryption
- Backups are sent offsite to a secure storage facility weekly

The SaaS hardware/software platform is implemented to be fault tolerant. As an SSAE 16 compliant data center, the data center is designed, tested and certified to withstand and function under disaster conditions without loss of service or data. Additionally, ClientTrack is designed to operate on readily available "commodity" server hardware and standardized Internet connection. In the extremely unlikely catastrophic event, our

disaster recovery plans enable the entire ClientTrack SaaS platform to be built from virtual servers in any data center unaffected by the catastrophe.

ClientTrack employs 24x7, a support model to address any needs associated with the server environment. This support is augmented on the ground in two separate geographically disperse locations with ViaWest's expert response teams. ClientTrack has experienced minimal downtime in the last 12 months and proactively works to ensure that remains the company standard.
The first step to resolving a reported problem is to isolate the problem as a network/ hardware problem or connectivity. ClientTrack employs a completely redundant network to allow a failover to occur without disruption to access. This normally rules out a network or hardware issue barring a catastrophic event. As outlined above, clients should immediately contact ClientTrack via the support line if connectivity is disrupted to allow immediate response. ClientTrack will immediately identify and resolve issues associated with access.
In the event of a catastrophic event, ClientTrack employs a series of disaster recovery procedures that are intended to identify possible threats so they can be addressed proactively. This includes a number of troubleshooting steps leading all the way up to activating the disaster recovery site to provide continuity of service. A catastrophic failure resulting in loss of connectivity will be recovered at the disaster recovery site within 4 hours. This allows the recovery network and data propagation to occur across all production environments in the second SSAE 16 facility.
ClientTrack reports any outage events including the cause, resolution, and mitigation steps employed to protect against a future outage. ClientTrack is designed to operate on readily available server hardware and standardized internet connections; in the extremely unlikely catastrophic event, the entire ClientTrack SaaS platform can be restored at a backup data center unaffected by the catastrophe.

Monitored Use

The HMIS Lead Agency may monitor Participating Agencies and any Authorized User's use of the Service and the Database, and Provider may freely use and disclose any information and materials received from any Authorized User or collected through Participating Agencies and Authorized User's use of the Service, including the Database and Content.

General
Participating Agency records shall be subject to audits, from time to time, that are consistent with the HUD regulations applicable to HMIS. It is the responsibility of the Participating Agency to present any applicable documents to the HMIS Lead Agency. At any time during normal business hours and as often as the HMIS Lead Agency, HUD, and/or any other government agency entitled to the Content of the Database may require and deem necessary, the Participating Agency shall make available all such records and documents as requested by said parties for audit and/or monitoring. The Provider, HUD, and/or applicable government agencies may examine and make excerpts or transcripts

from such records and may audit all contracts, procurement records, invoices, materials, personnel records, etc. relating to all matters covered by this Agreement.

HUD Performance Reviews and Monitoring
The Participating Agency understands that HUD may conduct performance reviews and monitoring of the HMIS implementation and of the Participating Agency in order to examine reported statistics, commitment rates, and compliance with eligibility, income targeting, and any other applicable requirements. The Participating Agency agrees to cooperate with HUD and the HMIS Lead Agency to undertake such remedial action as may be required pursuant to the HUD Regulations.

Monitoring by the HMIS Lead Agency
The HMIS Lead Agency may perform periodic monitoring of the Database and Participating Agency's use and entry of information into the same. The Participating Agency agrees to cooperate with the HMIS Lead Agency throughout any monitoring procedure and to implement such corrective action as requested.

In the event Monitoring is Not Performed
In the event that any monitoring or performance reviews are not conducted by the HMIS Lead Agency, HUD, and/or any other government agency, the Participating Agency shall not be excused from obligations to abide by all terms of this Agreement, all rules of HMIS Governance Charter and any HMIS or applicable HUD regulations.

Issue Severity Levels

Issues will be categorized and handled according to an assigned Severity Level. The Issue Severity Level is assigned by Eccovia Solutions, Inc. based upon initial triage processes.

Severity Level	Description	Response Times
Level 1 – Critical (Security Related)	The issue relates to the security of private data or the perception that private data may be available to unauthorized users.	1 hour
Level 2 – Urgent (Data Integrity)	The issue relates to the integrity of data being saved or viewed. No reasonable workaround is available.	1 hour
Level 3 – High (Availability)	The issue related to the availability of the Application, including all issues related to latency.	1 hour
Level 4 – Medium (Warranty)	The issue relates to a bug impacting normal use of the Application as it was intended or configured to perform.	1 business day
Level 5 – Medium (Information Request)	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; request for a System change.	2 business days

Support Escalation Table

- All Severity Level 1 and 2 issues should be escalated to the 3rd level of the Escalation Table at the time of Issue submission.

- All Severity Level 3 issues should be escalated to the 1st level of the Escalation Table at the time of Issue submission.
- Any Incident handling that does not achieve its objective response time for its Severity Level or for which a resolution plan is viewed as unsatisfactory by either party should be escalated to the next level, and to each successive escalation level until satisfaction is achieved.

Level	ClientTrack Resource	Licensee Resource
1st Level	Support Manager	Project Manager
2nd Level	Director-level Contact	Director-level Contact
3rd Level	Corporate Officer Contact	Corporate Officer Contact

Disposal

The City of Philadelphia contracts with a certified specialist for destruction of physical disk drives who can be utilized as required.

Encryption

The application is accessed by users via a secure HTTPS connection to the software web application server. The HTTPS protocol, which is designed to prevent eavesdropping and tampering, provides a secure communication channel to the application.

Hard Copy Security

The guidelines regarding the security of paper or other hard copy containing PPI that is either generated by or for the HMIS, including, but not limited to reports, data entry forms, and signed consent forms are:

1. HMIS Participating Agency or Look-Up Agency staff must supervise at all times any paper or other hard copy generated by or for the HMIS that contains PPI when the hard copy is in a public area.
2. Hard copy records containing PPI must be disposed of through means such as cross cut shredding and pulverizing.
3. When HMIS Participating Agency or Look-Up Agency staff is not present, the information must be secured in areas that are not publicly accessible.
4. Written information specifically pertaining to user access (e.g., User ID and password) must not be stored or displayed in any publicly accessible location.

ARTICLE 4: HMIS SECURITY PLAN APPENDICES

⇒ Information Security Policy Access Control
⇒ Information Security Policy Physical and Environmental Security
⇒ HMIS Vendor: Comprehensive Data Security, Privacy, and Confidentiality Policy and Plan for HIPAA
⇒ HMIS Vendor: Hosting and Security

ARTICLE 5: HMIS PRIVACY PLAN

The HMIS Participating Agencies (HPA) shall at all times comply with the HMIS Program Regulations in addition to all of the aforestated regulations, codes, statutes, laws, associated Executive Orders, OMB Circulars, other applicable Federal regulations, and all future revisions and amendments to the same. The Participating Agencies shall become thoroughly familiar with all of the foregoing requirements as applicable and shall ensure that the use of the Services complies in all respects.

A. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and all rules and regulations promulgated pursuant to the authority granted therein, including but not limited to, those set forth in 45 C.R.F. §§ 160-164 (2003), all as supplemented, replaced and amended from time to time.

B. Federal confidentiality regulations as contained in the Code of Federal Regulations, 42 C.F.R. 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 CFT Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose.

C. Pursuant to the HUD Data and Technical Standards Final Notice published in the Federal Register on March 29, 2010 and the PA-HMIS Governance Charter, each Participating Agency will prominently display a PA-HMIS Notice of Privacy Practices or a notice developed by the Participating Agencies that incorporates the content of the Continuum approved PA-HMIS Notice of Privacy Practices form, in its program offices where intake occurs, and will provide written copy of the Notices to all Clients enrolling in the Participating Agencies programs and services. The Subscriber will update its Notice of Privacy Practices as needed to comply with federal law and regulations and with the PA-HMIS policy changes.

Policy Access and Amendment

OHS may amend its privacy policy and practices at any time, subject to the recommendation of the CoC Board. The HMIS Lead Agency may bring issues to the CoC Board as necessary. An amendment may affect data that had been entered in the HMIS before the effective date of any such amendment. This policy is consistent with current privacy standards for HMIS issued by HUD. The provisions of this plan shall go into effect immediately.

Accountability

Each agency must uphold relevant Federal, State and Local confidentiality regulations and laws that protect client records, including but not limited to the privacy and security

standards found in HUD's Data and Technical Standards. If an HPA is covered by more stringent regulations, such as HIPAA, the more stringent regulations will prevail.

HMIS Data Disclosure and Use Limitations

The confidentiality of HMIS data will be protected. HMIS data may only be collected, used, or disclosed for activities described in this section. The HMIS Lead Agency requires that HPA notify individuals seeking their assistance that data collection, use, and disclosure will occur. By entering data into the designated HMIS System, the HPA verifies that individuals have provided the HPA with consent to use and disclose their data for purposes described below and for other uses and disclosures the HMIS Lead Agency determines to be compatible:

- To provide or coordinate individual referrals, case management, housing or other services. Client records may be shared with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information;
- For functions related to payment or reimbursement for services;
- To carry out administrative functions, including but not limited to audit, personnel oversight, and management functions;
- To produce aggregate-level reports regarding use of services;
- To produce aggregate-level reports for funders or grant applications;
- To create de-identified (anonymous) information;
- To track system-wide and project-level outcomes;
- To identify unfilled service needs and plan for the provision of new services;
- To conduct a study or research project approved by the CoC
- When required by law (to the extent that use or disclosure complies with and is limited to the requirements of the law);
- To avert a serious threat to health or safety if:
    - The use or disclosure is reasonably believed to be necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
    - The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
- To report about an individual reasonably believed to be a victim of abuse, neglect, or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect, or domestic violence in any of the following three circumstances:
    - Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
    - If the individual agrees to the disclosure; or
    - To the extent that the disclosure is expressly authorized by statute or regulation and either of the following is applicable:
        - The HPA believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
        - If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the

report represents that the HMIS data for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure;

- When such a permitted disclosure about a victim of abuse, neglect, or domestic violence is made, the individual making the disclosure will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:
  - In the exercise of professional judgment, it is believed that informing the individual would place the individual at risk of serious harm; or
  - It would be informing a personal representative (such as a family member or friend), and it is reasonably believed that the personal representative is responsible for the abuse, neglect, or other injury and that informing the personal representative would not be in the best interests of the individual as determined in the exercise of professional judgment.

- To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
  - In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
  - If the law enforcement official makes a written request for HMIS data that:
    - Is signed by a supervisory official of the law enforcement agency seeking the HMIS data;
    - States that the information is relevant and material to a legitimate law enforcement investigation;
    - Identifies the HMIS data sought;
    - Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
    - States that de-identified information could not be used to accomplish the purpose of the disclosure.
  - If it is believed in good faith that the HMIS data constitutes evidence of criminal conduct that occurred on the HPA' premises;
  - In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the HMIS data disclosed consists only of name, address, date of birth, place of birth, social security number and distinguishing physical characteristics; or
  - If the official is an authorized federal official seeking HMIS data for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), *and* the information requested is specific and limited in scope to

the extent reasonably practicable in light of the purpose for which the information is sought.

- To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.

The HMIS Lead may share client level HMIS data with HMIS participating entities as follows:

- The HPA originally entering or uploading the data to the designated HMIS.
- Outside organizations under contract with the HMIS Lead Agency or other entities acting on behalf of the HMIS Lead Agency for research, data matching, and evaluation purposes. The results of this analysis will always be reported in aggregate form; client level data will not be publicly shared under any circumstance.

Entities providing funding to organizations or projects required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by the HMIS Lead Agency when there is a voluntary written agreement in place between the funding entity and the organization or project. In such cases, funder access to HMIS will be limited to data on the funded organization or project. Funding for any organization or project using HMIS cannot be contingent upon establishing a voluntary written agreement allowing the funder HMIS access.

Any requests for reports or information from an individual or group who has not been explicitly granted access to the Philadelphia CoC HMIS will be directed to the HMIS System Administrator. No individual client data will be provided to meet these requests without proper authorization.

Before any use or disclosure of PII that is not described here is made, the HMIS Lead Agency or HPA wishing to make the disclosure will seek the consent of all individuals who's PII may be used or disclosed.

Confidentiality

Each agency must maintain any/all personal information as required by federal, state, or local laws.

Each agency shall only solicit or input into HMIS client information that is essential to providing services to the client.

Each agency shall not knowingly enter false or misleading data under any circumstance, nor use HMIS with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.

Each agency shall ensure that all staff, volunteers and other persons who use HMIS are issued an individual User ID and password by OHS.

Each agency shall ensure that all staff, volunteers and other persons issued a User ID and password for HMIS receive confidentiality training, HMIS training, and comply with the attached *HMIS User Agreement* and the *HMIS Participation Agreement*.

Protections for Victims Of Domestic Violence, Dating Violence, Sexual Assault, And Stalking

Victim service providers are prohibited from entering data into HMIS. Other agencies must be particularly aware of the need for confidentiality regarding information about persons who are victims of domestic violence, dating violence, sexual assault, and stalking. Additional protections for these clients include explicit training for staff handling personal identifying information of the potentially dangerous circumstances that may be created by the improper release of this information.

No Unauthorized Access

Participating Agencies shall not permit unauthorized access to the Service or any of the Content. Neither Participating Agencies nor any of its Sub-Contractors shall permit their clients, customers, vendors, consultants, service providers, agents, contractors, subcontractors, business partners, consortium partners, joint venture partners, affiliates (other than wholly owned subsidiary), concessionaires, subscribers, members, or associative/cooperative members or employees thereof access to the Service, Content, or any portion of the Database or Information, other than as may be expressly permitted herein. The Participating Agency shall immediately notify HMIS Administrator upon learning of any unauthorized access, or the actual or potential compromise or breach of any security measures related to the Service or Content.

Personal Information

Medical or personal information of individuals may be in the Database, or otherwise contained or entered into the Content ("Personal Information"). Some or all of the Personal Information may be subject to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, or other state or federal laws providing protection and safe guards for relevant Personal Information ("Privacy Laws"). Subscriber shall ensure that it is familiar with any applicable Privacy Laws, and shall be responsible for ensuring that no violation of those Privacy Laws occurs through Participating Agency's use of the Service. The HMIS Lead Agency shall take reasonable actions and endeavor to comply with all Privacy Laws, but the HMIS Lead Agency is not responsible for the breach of any Privacy Laws by the Participating Agency, or any other participating agency and the information that they may add to the Content and Database. Upon being notified of any violation or potential violation of Privacy Laws, The HMIS Lead Agency will take such reasonable actions as it deems necessary and fit to remain compliant with the Privacy Laws.

Inter-Agency Data Sharing

Policy: *The HMIS is an "open" system, meaning that data can be shared between HMIS participating agencies. Whether data is actually shared or not is determined on a per client basis, based on user input and client data sharing preferences.*

If the client elects to have their information shared partially or completely, and the agency with the initial service begins working with another agency not participating in HMIS, then those agencies must use either the Inter-Agency Partnership Data Sharing Agreement or develop a Memorandum of Understanding.

Explanation: The need for client confidentiality and the benefit of integrated case management needs be balanced. For the purposes of fulfilling regulations and community needs, the position to share information electronically is in favor. HMIS has been designed to permit Inter-Agency data sharing while still safeguarding client confidentiality.

Procedure: When new clients are entered into HMIS, the initiating user must set the Client's data sharing permission (called a data sharing policy, based on the Client's response on the Authorization to Consent form) before data sharing is permitted. These permissions control the information that is shared about the client globally. If no data sharing policy is set up, HMIS assumes that data sharing is not permitted.
Users must record the actual responses received by the client when setting up the client's electronic data sharing policy. Users may be monitored to ensure compliance with this policy at any time by Agency Managers, HMIS Leads, or the HMIS System Administrator, in which case users will need to provide a copy of any Authorization to Consent forms that are requested. Any user found to not adhere to the data sharing permissions allowed by the client will be immediately and permanently banned from HMIS, and may face possible legal action. If a user feels it is in the best interest of the client, they may further restrict the information that is shared by disallowing extra data elements in the client's electronic sharing policy, but users may never choose to implement a less restrictive data sharing policy without collecting a new Authorization to Consent form that has been signed by the client and permits less restrictive data sharing.

Ethical Data Use

Policy: *Data contained in the HMIS will only be used to support or report on the delivery of homeless and housing services in the City of Philadelphia. Each HMIS User will affirm the principles of ethical data use and client confidentiality contained in the HMIS Policies and Standard Operating Procedures Manual, the HMIS Participation Agreement, and the HMIS System User Agreement. Each Authorized Agency must have a written privacy policy, including specific policies related to employee misconduct or violation of client confidentiality. All HMIS Users must understand their Agency's privacy policy, and a signed policy statement must become a permanent part of the employee's personnel file.*

Procedure: All HMIS users will sign a HMIS System User Agreement before being given access to the HMIS. Any individual or Authorized Agency misusing, or attempting to misuse HMIS data will be denied access to the database, and their relationship with

HMIS Lead Agency may be terminated. Any Authorized Agency for which the relationship with HMIS Lead Agency is terminated will also likely have funds reallocated by OHS because of the statutory requirement to participate in the Continuum's HMIS.

Access to Core Database

Policy: *No one but OHS staff will have direct access to the HMIS database through any means other than the HMIS user interface, unless explicitly given permission by OHS during a process of software upgrade, conversion, or for technical assistance.*

Procedure: EccoVia, Inc. and OHS staff will monitor both our web application server and our database server and employ updated security methods to prevent unauthorized database access.

Client Rights and Confidentiality of Records

Policy: *HMIS operates under a protocol of inferred consent to include client data in the HMIS. Each Authorized Agency is required to post a sign about the privacy policy in a place where clients may easily view it (i.e. - at the point of intake, on a clipboard for outreach providers, in a case management office). The privacy posting should include a statement about the uses and disclosures of client data as outlined in this document. Written authorization for inclusion of a client's data in HMIS is not required, but is inferred when a client accepts the services offered by the program and when the privacy posting is displayed for client review.*

Clients may opt out of HMIS or be able to provide basic personal information. Clients have the right of refusal to provide personal identifying information to the HMIS, except in cases where such information is required to determine program eligibility or is required by the program's funders. Such refusal or inability to produce the information shall not be a reason to deny eligibility or services to a client. When a client exercises their right of refusal, de-identified demographic (anonymous) information will be entered into the HMIS.

Each Authorized Agency shall take appropriate steps to ensure that authorized users only gain access to confidential information on a "need-to-know" basis in accordance with this document and their own Privacy Policy. Duly authorized representatives of OHS may inspect client records (including electronic records) at any time, although non-HMIS staff will not, as a matter of routine, be permitted to access protected private information. OHS and Authorized Agencies will ensure the confidentiality of all client data as described in this document.

Explanation: The data in the HMIS is personal data, collected from people in a vulnerable situation. OHS and Authorized Agencies are ethically and legally responsible to protect the confidentiality of this information. The HMIS will be a confidential and secure environment protecting the collection and use of client data.

Procedure: Access to client data will be controlled using security technology and restrictive access policies. Each Authorized Agency must develop and make available a privacy policy related to client data captured in HMIS and through other means. A posting that summarizes the privacy policy must be placed in an area easily viewed by clients, and must also be placed on the Authorized Agency's web site (if they have one). Only individuals authorized to view or edit individual client data in accordance with the stated privacy policies and these Standard Operating Procedures will have access to that data. The HMIS will employ a variety of technical and procedural methods to ensure that only authorized individuals have access to individual client data.

Each agency must allow individuals to inspect and have a copy of their personal information that is maintained in HMIS.

Each agency must offer to explain any information that is not understood.

Individuals must submit a request to inspect their HMIS data in writing to their social worker/case manager. Each agency must consider a written request for correction of inaccurate or incomplete personal information. If the agency agrees that the information is inaccurate or incomplete, the agency may delete it or may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
Each agency may deny the individual's request for inspection or copying of personal information if:

a. Information was compiled in reasonable anticipation of litigation or comparable proceedings
b. Information is about another client/consumer
c. Information was obtained under a promise of confidentiality and the disclosure would reveal the source of the information, or
d. Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If the agency denies a request for access or correction, it must explain the reason for the denial and include documentation of the request and the reason for the denial.

Each agency may reject repeated or harassing requests for access or correction.

Authorized Agency Grievances

Policy: *Authorized Agencies will contact the HMIS System Administrator to resolve HMIS problems including but not limited to operation or policy issues. If an issue needs to be escalated, the HMIS System Administrator may contact OHS's Law Office. OHS, through the HMIS System Administrator, will have final decision-making authority over all grievances that arise pertaining to the use, administration, and operation of the HMIS.*

Procedure: Users at Authorized Agencies will bring HMIS problems or concerns to the attention of their Agency Manger. If problems, concerns, or grievances cannot be addressed by the Agency Manager, the Agency Manager will contact the HMIS System

Administrator, who may ask for these issues to be stated in writing. If it is not appropriate to raise the issue with the Agency Manager, users may contact the HMIS System Administrator directly via phone, email, or mail. If the grievance requires further attention, the HMIS System Administrator may consult with OHS's Law Office. OHS, through the HMIS System Administrator, shall have final decision-making authority in all matters regarding the HMIS.

Client Grievances

Policy: *Clients must contact the Authorized Agency with which they have a grievance for resolution of HMIS problems or the Homeless Consumer Response Line (HCRL). Authorized Agencies will report all HMIS-related client grievances to the HCRL. If the Authorized Agency's grievance process has been followed without resolution, the Authorized Agency may escalate the grievance to the HCRL as outlined in the "Authorized Agency Grievances" section. At any time, clients may request that their personally-identifying information be removed from the HMIS.*

Procedure: Each Authorized Agency is responsible for answering questions, complaints, and issues from their own clients regarding the HMIS. Authorized Agencies will provide a copy of their privacy policy and/or copies of the HMIS Privacy Policy upon client request. Client complaints should be handled in accordance with the Authorized Agency's internal grievance procedure, and then escalated to the HCRL in writing if no resolution is reached. OHS is responsible for the overall use of the HMIS, and will respond if users or Authorized Agencies fail to follow the terms of the HMIS agency agreements, breach of client confidentiality, or misuse of client data. Authorized Agencies are obligated to report all HMIS-related client problems and complaints to the HMIS System Administrator, who will determine the need for further action. Resulting actions might include further investigation of incidents, clarification or review of policies, or sanctioning of users and Agencies if users or Agencies are found to have violated standards set forth in HMIS Participation Agreements or the HMIS Governance Charter. Upon the client's request for data removal from the HMIS, the Agency Manager will delete all personal identifiers of client data within 24 hours. A record of these transactions will be kept for a period of three years by the Agency Manager and provided to OHS upon request.

Authorized Agency Hardware/Software Requirements

Policy: *Authorized Agencies will provide their own computer and method of connecting to the Internet, and thus to the HMIS.*

Procedure: Contact the HMIS System Administrator for the current status of assistance.

Hardware/Software Requirements: HMIS is web-enabled software; all that is required to use the database is a computer, a valid username and password, and the ability to connect to the Internet using internet browser software (Google Chrome, Firefox, etc.). There is no unusual hardware or additional HMIS-related software or software installation required. OHS recommends the following workstation specifications.

Minimum Workstation Requirements

- Computer: PC 500 MHz or better
- Web Browser: Microsoft Internet Explorer 5 or higher, Mozilla Firefox 3.0 or higher, Google Chrome 4.0.249 or higher, or Netscape Navigator 6.0 or higher
- Hard Drive: 2 GB
- 64 MB RAM
- Internet Connectivity (broadband or high-speed)
- SVGA monitor with 800 x 600+ resolutions
- Keyboard and Mouse

Recommended Workstation Requirements

- Computer: 1 Gigahertz Pentium Processor PC
- Browser: Google Chrome v.41 or higher, Mozilla Firefox 29.0 or higher, Internet Explorer 11 or higher, or Safari 5.1.10
- 20 GB Hard Drive
- 512 MB RAM
- Broadband Internet Connection - 128 Kbps (hosted version) or LAN connection
- SVGA monitor with 800x600 + resolution
- Keyboard and mouse

Although there is no unusual hardware or additional HMIS-related software required to connect to the database, the speed and quality of the Internet connection and the speed of the hardware and could have a profound effect on the ease of data entry and report extraction. DCED also recommends the use of Windows 7 or higher (1 GHz models or faster) as the Windows platform to eliminate certain technical problems and a high-speed Internet connection.

ARTICLE 6: HMIS PRIVACY PLAN APPENDICES

⇒ Notice Of Privacy Practices
⇒ Consumer Notice
⇒ Authorization To Disclose Client Information
⇒ Information Request Form
⇒ Acknowledgement Form

ARTICLE 7: Governing Regulation

This Privacy and Security Plan shall be governed by and interpreted for any and all purposes in accordance with the "Department of Housing and Urban Development Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice," July 30, 2004, including subsequent revision. In the event of any discrepancy between the two documents, the latter shall prevail.

ARTICLE 8: Duration

This plan must be reviewed annually and updated as needed by the HMIS Lead Agency on behalf of the Philadelphia Continuum of Care.

Update Log

Created:	January 21, 2014
Reviewed and Reapproved:	March 18, 2015
	August 29, 2016
	September 11, 2017
	May, 2019