Hampden County HMIS • Springfield Office of Housing

SECURITY PLAN

Security Officers

The Springfield Office of Housing has designated an HMIS Security Officer whose duties include:

- Review of the Security Plan annually and at the time of any change to the security management process, the data warehouse software, the methods of data exchange, and any HMIS data or technical requirements issued by HUD. In the event that changes are required to the HMIS Security Plan, the Security Officer will work with the HMIS and Data Committee for review, modification, and approval.
- Confirmation that the Springfield Office of Housing adheres to the Security Plan.
- Response to any security questions, requests, or security breaches to the Hampden County HMIS and communication of security-related HMIS information to CHOs.

Each CHO must also designate a CHO HMIS Security Officer whose duties include:

- Confirmation that the CHO adheres to the Security Plan.
- Communication of any security questions, requests, or security breaches to the Hamden County CoC HMIS Security Officer, and security-related HMIS information relayed from the Hampden County HMIS System Administrator to the CHO's end users.
- Participate in security training offered by the City of Springfield.

Annual Security Certification

The Springfield Office of Housing and each CHO must complete an annual security review to ensure the implementation of the security requirements for the HMIS. This security review must include completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan. Each CHO Security Officer must complete the Security Self-Certification each January using the attached form and submit the completed form to the CoC Security Officer no later than February 15 of each year.

Security awareness training and follow-up

All users must receive security training prior to being given access to the HMIS. The Springfield Office of Housing has created an on-line security and privacy training module which must be completed prior to being issued a password. The request for new password requires a certification that the new user has completed the on-line training. In addition, the Springfield Office of Housing shall provide security training no less than once per year.

Reporting security incidents

The HMIS Lead has created the following policy and chain of communication for reporting and responding to security incidents.

Security Incidents

All HMIS users are obligated to report to their agency HMIS Security Officer suspected instances of noncompliance with policies and procedures that may leave HMIS data vulnerable to intrusion. Each CHO is responsible for reporting any security incidents involving the real or potential intrusion of the Hampden County HMIS to the Springfield Office of Housing. The Springfield Office of Housing is responsible for reporting any security incidents involving the real or potential intrusion of the Hampden County HMIS to the Hampden County CoC Steering Committee.

Reporting Threshold

HMIS users must report any incident in which unauthorized use or disclosure of PII has occurred and any incident in which PII may have been used in a manner inconsistent with the CHO Privacy or Security Policies. Security breaches that have the possibility to impact the Hampden County HMIS must be reported to the HMIS Administrator.

Reporting Process

HMIS users will report security violations to their CHO HMIS Security Officer. The CHO HMIS Security Officer will report violations to the Springfield Office of Housing HMIS Security Officer. Any security breaches identified by Social Solutions ETO will be communicated to the Springfield Office of Housing Security Officer and System Administrator. The System Administrator will review violations and recommend corrective and disciplinary actions to the HMIS and Data Committee and the Steering Committee, as appropriate. Each CHO will maintain and follow procedures related to internal reporting of security incidents.

Audit Controls

Social Solutions maintains an accessible audit trail within ETO that allows the Hampden County HMIS Administrator to monitor user activity and examine data access for specified users. The Hampden County HMIS Administrator will monitor audit reports for any apparent security breaches or behavior inconsistent with the Privacy Policy outlined in these policies and procedures. In addition, CHO Site Managers are required to run audit reports on all HMIS user staff two times per year and submit these audit reports to the Hampden County HMIS Administrator.

System Security

Each 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.

User Authentication

A CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Virus Protection

A CHO must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

Firewalls

A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall as long as the server has a firewall.

Physical Access to Systems with Access to HMIS Data

A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff is not present, steps should be taken to ensure that computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.

Hard Copy Security

A CHO must secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PII when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.

Hard copies of data stored or intended to be stored in HMIS, regardless of whether the data has yet been entered into HMIS, will be treated in the following manner:

1. Records shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, records shall be maintained in such a manner as to prevent exposure of PII to anyone other than the user directly utilizing the record.
3. Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the CHO's place of business and where return of the records by the close of business of would result in the undue burden on staff.
4. When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not re-disclose the PII contained in those records except as permitted by these policies and procedures.
5. Faxes or other printed documents containing PII shall not be left unattended.
6. Fax machines and printers shall be kept in secure areas.
7. When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
8. When finished faxing, copying or printing all documents containing PII should be removed from the machines promptly.

Database Integrity

The CHO must not intentionally cause corruption of the Hampden County HMIS in any manner. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, will result in immediate suspension of HMIS licenses held by the CHO, and suspension of continued access to the Hampden County HMIS by the CHO.

The City will investigate all potential violations of any security protocols. Any user found to be in violation of security protocols will be subject to sanctions, as described in the HMIS Policies and Procedures Manual. Individual users may be subject to disciplinary action by the employer CHO.

Disaster Recovery

Hampden County HMIS data is stored by Social Solutions in secure and protected off-site locations with duplicate back-up. In the event of disaster, the HMIS Administrator will coordinate with Social Solutions to ensure the HMIS is functional and that data is restored. The Springfield Office of Housing will communicate to CHOs when data becomes accessible following a disaster.

Contracts and other arrangements

The HMIS Lead shall retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or required to comply with HUD requirements for a five-year period.

Hampden County HMIS
CHO Security Certification

Identification of Security Officer

Organization Name

Security Officer

Name

Title

Phone

Email

Security Officer duties include, but are not limited to:

- Annually review the Security Certification document and test the CHO security practices for compliance.
- Using this Security Certification document, certify that the CHO adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time. Communicate any security questions, requests, or security breaches to the Hampden County HMIS System Administrator and Security Officer.
- Communicate security-related HMIS information to the organization's end users.
- Complete security training offered by the HMIS Lead.
- Additional duties specified in the HMIS Participation Agreement.

CHO Security Officer signature indicating understanding and acceptance of these duties:

_____

Signature Date

Each organization is required to meet the following security requirements. If the requirement cannot be met at the time of the initial certification, you must indicate a date not later than three months after the initial certification by which you will have met the requirement. At that time, you will be required to submit an updated version of this form demonstrating your compliance.

	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
User Authentification	Does the agency abide by the HMIS policies for unique user names and password?	All HMIS users at the agency are aware that they should: ___ Y ___ N NEVER share username and passwords ___ Y ___ N NEVER keep usernames/ passwords in public locations ___ Y ___ N NEVER use their internet browser to store passwords ___ Y ___ N All users have signed a receipt of compliance for staff	
Hard Copy Data	Does agency have procedures in place to protect hard copy Personal Protected Information (PPI) generated from or for the HMIS?	Agency has procedure for hard copy PPI that includes: (1) Security of hard copy files ___ Y ___ N Locked drawer/file cabinet ___ Y ___ N Locked office (2) Procedure for client data generated from the HMIS ___ Y ___ N Printed screen shots ___ Y ___ N HMIS client reports ___ Y ___ N Downloaded data into Excel ___ Y ___ N Copy of above procedures is available ___ Y ___ N Agency trains all staff on hard copy procedures	
PPI Storage	Does the agency dispose of or remove identifiers from a client record after a specified period of time? (Minimum standard: 7 years after PPI was last changed if record is not in current use.)	___ Y ___ N Agency has a procedure Describe procedure: _____ _____	

Virus Protection	Do all computers have virus protection with automatic update? (This includes non-HMIS computers if they are networked with HMIS computers.)	Virus software and version _____ ___ Y ___ N Auto-update turned on Date last updated: ____ / ____ / _____ Person responsible for monitoring/updating: _____	
Firewall	Does the agency have a firewall on the network and/or workstation(s) to protect the HMIS systems from outside intrusion?	Single computer agencies: ___ Y ___ N Individual workstation Version: _____ Networked (multiple computer) agencies: ___ Y ___ N Network firewall Version: _____	
Physical Access	Are all HMIS workstations in secure locations or are they manned at all times if they are in publicly accessible locations? (This includes non-HMIS computers if they are networked with HMIS computers.)	All workstations are: ___ Y ___ N In secure locations (locked ofcs) or manned at all times ___ Y ___ N Using password protected screensavers All printers used to print hard copies from the HMIS are: ___ Y ___ N In secure locations Data Access: ___ Y ___ N Users may access HMIS from outside the workplace ___ Y ___ N If yes, Agency has a data access policy	
Data Disposal	Does the agency have policies and procedures to dispose of hard copy PPI or electronic media?	___ Y ___ N Agency shreds all hardcopy PPI before disposal Before disposal, the Agency reformats/degausses (demagnetizes): ___ Y ___ N Disks ___ Y ___ N CDs ___ Y ___ N Computer hard-drives ___ Y ___ N Other media (tapes, jump drives, etc)	

Software Security	Do all HMIS workstations have current operating system and internet browser security? (This includes non-HMIS computers if networked with HMIS computers.)	Operating System (OS) Version: _____ ___ Y ___ N All OS updates are installed ___ Y ___ N Most recent version of Internet Browser(s) are installed	

We affirm and certify the above information is true and that this organization, _____, is in full compliance with all requirements listed as "CHO" (Contributing HMIS Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the Hampden County HMIS Policies and Procedures or will be in compliance within the timeframes stated above. This certification is incorporated into the HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

HMIS Security Contact

Signature

Date

Executing Officer

Signature

Date