Massachusetts Balance of State Continuum of Care

HMIS Security Plan

Security refers to the protection of client Protected Identifying Information (PII) and sensitive program information from unauthorized access, use, or modification.

Security Plan Purpose

Security standards as provided in this plan are directed to ensure the confidentiality, integrity, and availability of all Homeless Management Information System (HMIS) data; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users. Written policies and procedures must comply with all applicable Federal law and regulations, and applicable state or local governmental requirements.

Applicability

This plan applies to all Agencies accessing data contained in, generated from, or created for MAHMIS, including but not limited to: the Massachusetts Department of Housing and Community Development (DHCD), the Balance of State CoC's HMIS Lead (currently DHCD), all other CoCs, organizations providing services to homeless persons or those at risk of homelessness, Covered Homeless Organizations (CHOs), and the HMIS Vendor, hereafter collectively referred to as "Covered Homeless Organization" or "CHO." Each of these CHOs must follow all the security standards established in this notice. A CHO must comply with Federal, state, and local laws that require additional privacy or confidentiality protections. When a privacy or security standard conflicts with other Federal, state, and local laws to which the CHO must adhere, the CHO must adhere to the most stringent law or policy.

Administrative Safeguards

Security Officer

Each CoC HMIS Lead and each Agency/CHO must designate an HMIS Security Officer to be responsible for ensuring compliance with applicable security standards and provide the name and contact information to DHCD HMIS Staff.

Workforce Security

The CHO will be responsible for keeping a record of all end-user/staff agreements, privacy and ethics training sign-offs, Criminal Offender Record Information ("CORI") checks, and any other applicable records on site. The CHO's Executive Director or authorized signatory will designate one CHO HMIS Administrator who will assume responsibility for the creation and maintenance of projects and user accounts, as well as for providing and documenting the security training of any staff person prior to issuance of a user account. Said designee will be identified to DHCD HMIS Staff upon designation and when the designee changes.

A CHO's Human Resources department must put into place processes for promptly notifying the CHO's HMIS Administrator upon termination of employment to facilitate prompt deactivation of End User accounts.

MAHMIS Security Awareness Training and Follow-up

All MAHMIS end users must read the Security Policies and Procedures document governing HMIS and sign off on an acknowledgement form prior to being given access to MAHMIS. Security training will be conducted at least annually.

Reporting a Security Breach

Chain of Communication

HUD will later provide a defined threshold when reporting is mandatory. DHCD has two documents regarding security incidents: **Enterprise IT Security Incident Response Policy** and **Enterprise Security Incident Handling Procedures**.

Security Plan Noncompliance

Failure to comply with the Security Plan or the Security Policies and Procedures by an End User or a CHO will result in the immediate suspension of access to MAHMIS by DHCD until the allegations are resolved in order to protect the integrity of the system.

Security Breaches

If there is a suspected security breach involving any client PII, DHCD is to be contacted immediately. DHCD will take immediate action to mitigate the breach and notify DHCD's legal department, which will ensure compliance with the Commonwealth's Identity Theft Law, M.G.L., Ch 93H.

Disaster Recovery Plan

HUD has not yet established requirements for this. DHCD has a disaster recovery plan titled **Disaster Recovery Plan** dated November 2014. The HMIS Vendor's Disaster Recovery Plan is on file with DHCD. *Those plans should be referenced and include protocols for communication with staff, the CoC, and AGENCIES. Double-check re: state law, do all agencies need one?*

Annual Security Review

Annually, DHCD will complete and document a security review to ensure the implementation of the security requirements for itself. The Security Officer of each CHO will complete and document a security review to ensure the implementation of the security requirements for itself.

Contracts and Other Arrangements

DHCD will retain copies of all contracts and agreements executed as part of the administration and management of MAHMIS.

Technical Safeguards

System Security

System security provisions will apply to all systems where PII is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, tablets, smart phones, mainframes, and servers.

Internal Security Practices

Each CHO must establish and abide by a Written Information Security Policy, including identifying a Security Officer. The CHO's formal policies and procedures for terminating employment must include the notification of the CHO's MAHMIS Administrator, who will then be responsible for immediately disabling the End User's MAHMIS account.

Connectivity and Computer Systems

CHOs will connect to the Balance of State CoC's HMIS independently via the internet and are responsible for providing their own internet connectivity and computer systems sufficient for doing so.

CHOs must only access the HMIS using computers with operating systems, web browsers, and other software that are currently supported by their manufacturer and have not reached end-of-life.

Workstation Security

At a minimum, the primary workstation used by each End User to log in to HMIS should [insert more general language for plan, must maintain virus detection software and firewalls]

- Password-protected log on for the workstation itself;
- Password-protected (aka locked) screensaver after five minutes of inactivity;
- Operating system updated with the manufacturer's latest patches at least weekly. No operating systems that have reached end-of-life are to be used under any circumstances;

- Ports firewalled;
- Use the most up-to-date internet browser that is compatible with the HMIS application
- System scanned at least weekly for viruses and malware.

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.

Firewalls

A CHO must protect its 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 gateway would not need a firewall as long as the gateway has a firewall. Firewalls are commonly included with all new operating systems. Older operating systems can be equipped with secure firewalls that are available both commercially and for free on the Internet.

Public Access

HMIS that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates, or extranets that limit access based on the Internet Protocol (IP) address, or similar means. A public forum includes systems with public access to any part of the computer through the Internet, modems, bulletin boards, public kiosks or similar arenas. Further information on these tools can be found in the HMIS Consumer Guide and the HMIS Implementation Guide, both available on HUD's Web site.

Disposal

In order to delete all HMIS data from a data storage medium, a covered homeless organization must reformat the storage medium. The CHO should reformat the storage medium more than once before reusing or disposing the medium.

System Monitoring

CHOs must use appropriate methods to monitor security systems. Systems that have access to any HMIS data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely.

HMIS Security

Applicability

A CHO must apply application security provisions to the software during data entry, storage and review or any other processing function.

User Authentication

A CHO must secure all electronic HMIS data with, at a minimum, a user authentication system consisting of a unique username and a password.

Under no circumstances shall a CHO demand that an End User hand over his or her username and password.

Under no circumstances shall an End User share their HMIS login information.

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 should 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.

End users must log off of the HMIS when complete.

Electronic Data Transmission

A CHO must encrypt all HMIS data that are electronically transmitted over the Internet, publicly accessible networks, or phone lines to current industry standards. Unencrypted data may be transmitted over secure direct connections between two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data. A secure network would have secure direct connections. The Commonwealth maintains a secure server which must be used to electronically transmit any data using PII between a CHO and any employee of the Commonwealth of Massachusetts.

Electronic Data Storage

CHO users are responsible for maintaining the security and confidentiality of any program participant-level data extracted from the database and stored locally, including all data used in internal reporting. No identifiable program participant-level data is to be transmitted unless it is properly protected. Security questions should be addressed to HMIS Project Staff.

Remote System Access

CHOs and their End Users must abide by these Policies and Procedures and ensure the security and confidentiality of program participant data regardless of the computer used to log in to the system. For this reason, End Users are prohibited from extracting and storing Protected Identifying Information (PII) on their personal computers and internet devices. End Users are prohibited from accessing the HMIS using public Wi-Fi.

Physical Safeguards

Physical Access to Systems with Access to HMIS Data:

A CHO must at all times staff computers stationed in public areas that are used to collect and store HMIS data. When workstations are not in use and staff are not present, steps should be

taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a period of inactivity, users will be automatically logged off of the HIMIS application. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by a CHO. 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 Protected Identifying Information that is 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 are not present, the information must be secured in areas that are not publicly accessible.

Remote Work

CHOs with remote work policies must make sure that the policies comply with all conditions in this and any other security and privacy documents issued by the CoC.

Applicable Laws

All applicable laws must be followed. These can include, but are not limited to:

Federal Laws

- Federal Register Vol. 69, No. 146 (HMIS FR 4848-N-02) (Federal statute governing HMIS information);
- 42 CFR Part 2 (Confidentiality Of Substance Use Disorder Patient Records)
- Health Insurance Portability and Accountability Act (HIPAA)

Massachusetts State Laws

- 201 CMR 17.00 (Standards for the Protection of Personal Information of MA Residents)
- Chapter 66 (Fair Information Practices)
- Chapter 93 (Security Breaches)
- Executive Order 504 (Security and Confidentiality of Personal Information)