Section 4- Security Plan

Introduction to the HMIS Security Plan

HMIS security standards are established to ensure the confidentiality, integrity and availability of all HMIS information. The security standards are designed to protect against any reasonably anticipated threats or hazards to security and must be enforced by system administrators, agency administrators as well as end users. This section is written to comply with section 4.3 of the 2004 Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice (69 Federal Register 45888) as well as local legislation pertaining to maintaining an individual's personal information. In December 2013, HUD released proposed regulations pertaining to HMIS Security. These regulations are not yet in force and sufficient guidance has not been given to enact the policies.

Meeting the minimum standards in this Security Plan is required for participation in the HMIS. Any agency may exceed the minimum standards described in this plan and are encouraged to do so. All Agency Data Administrators are responsible for understanding this policy and effectively communicating the Security Plan to individuals responsible for security at their agency.

Security Plan Applicability

The HMIS System and all agencies must apply the security standards addressed in this Security Plan to all the systems where personal protected information is stored or accessed. Additionally, all security standards must be applied to all networked devices. This includes, but is not limited to, an agency's networks, desktops, laptops, mobile devices, mainframes and servers.

All agencies, including the HMIS Lead, will be monitored by the HMIS System Administrators annually to ensure compliance with the Security Plan. Agencies that do not adhere to the security plan will be given a reasonable amount of time to address any concerns. Egregious violations of the security plan may result in immediate termination of an agency or user's access to the HMIS as determined by the HMIS Lead.

System Security

User Authentication

Agency Data Administrators and System Administrators shall limit access to those who meet each of the following –

1. Access is required for the purpose of data assessment, entry, or reporting
2. New User Training has been completed including the Standard Operating Procedures, Agency Privacy Policies, the Standard Workflow, and the overall HMIS software orientation.
3. User is covered by the agency privacy notice
4. User has signed and agreed to the HMIS End User Policy and Code of Ethics.

5. Have an agency email address to ensure HMIS access is granted to active employees only. Publicly available domain names are not appropriate (gmail.com, Hotmail.com, etc.) unless the agency uses these domain names as their agency standard.

It is the responsibility of Agency Data Administrators to immediately inactivate a user and notify System Administrators when the person leaves the agency or no longer requires access to the HMIS. Users who have not successfully logged into HMIS for 30 or more days may be inactivated by the System Administrator to further assure that access is only granted to those who require it.

The HMIS System only permits users to be logged into HMIS from one workstation or device at any given time.

User access and user access levels will be determined by the System Administrator in consultation with the Agency Data Administrator. The roles and responsibilities pertaining to assignment and creation of user licenses are outlined in *Section 1: Roles and Responsibilities*.

Each user must have a unique user ID. Each user's identity will be authenticated using a user password. Passwords are the individual's responsibility. **Users are prohibited from sharing user IDs or passwords.** A temporary password will be automatically generated from the system when a new user is created. Agency Data Administrators or System Administrators will communicate the system-generated password to the user. The user will be asked to establish a permanent password at initial log-in.

Users must select and change their own passwords every forty-five days. A password cannot be consecutively re-used. Password format is case-sensitive and must be between eight and sixteen characters long including at least two numbers and not be easily guessed. Any passwords written down must be securely stored and inaccessible to other persons. If a user unsuccessfully attempts to logon three times, the user ID will be "locked out", access permission revoked, and the user will be unable to gain access until their password is reset.

Agency Data Administrators and System Administrators have permission to reset a user's password. Users may submit a Help-Desk request for assistance, www.dupageco.org/HMISHelp.

Virus Protection

All devices directly accessing the HMIS and any device that is on a network that has a device directly accessing the HMIS must have industry compliant virus protection software installed. Both Operating System updates and virus definitions must be set to be updated and applied automatically. The virus protection software must also include anti-spyware functionality. Operating Systems must be supported by their vendors. Virus scans must be completed at least weekly.

Firewalls

An agency must protect the HMIS and client data from malicious intrusion behind a secure and up-to-date firewall. Each individual device does not need its own firewall, as long as there is a firewall between that device and any systems, including the Internet and other computer networks, located outside of the organization. For example, a device that accesses the Internet through a modem, public Wi-Fi or cellular data network would need its own firewall. A device that accesses the Internet through a central server would not need a firewall as long as the server has a firewall. Firewalls are commonly included with all new operating systems.

Physical Access

All computers and devices must be controlled through physical security measures and/or a password.
Users must logoff from the HMIS and their device if they leave their workstation. The HMIS System automatically logs users off after 30 minutes of inactivity. When devices are not in use, a password protected screensaver or lock screen should automatically turn on within 15 minutes of inactivity. Users on mobile devices or working in outreach locations in addition to system administrators are encouraged to decrease this time to 5 minutes.

Users should be trained on how to quickly lock their computer or device if they need to step away. On windows workstations, this is achieved by typing the command “Windows Key + L.” Different operating systems have different locking mechanisms.

If users are going to be away from the computer or device for an extended period of time they are encouraged to shut down the computer or device. Users should follow their agency’s “shut-down procedures” to ensure proper device, network, and virus updates.

Disposal

Agency policies, consistent with applicable state and federal laws, should be established regarding appropriate locations for storage, transmission, use and disposal of HMIS generated hardcopy or digital data. Reasonable care should be used, and media should be secured when left unattended. Magnetic media containing HMIS data which is released and/or disposed of from the participating organization and central server should first be processed to destroy any data residing on that media. Degaussing and overwriting are acceptable methods of destroying data.

System Monitoring

The HMIS maintains a permanent audit trail that tracks user log-in attempts and modifications to client records. Each audit entry reflects the user that created the entry and the date and name of the user that made the most recent modification.

These user logs will be checked routinely according to best practices established by the HMIS Lead Agency. Possible mechanisms the HMIS Lead may utilize are comparing the volume of search records accessed compared to the size of the agency, looking for multiple user logins from multiple locations, client searches occurring without record adjustment, users logging into the system at strange times and looking at the frequency of user password reset and lockout.

Hard Copy Data

Printed versions (hardcopy) of confidential data should not be left unattended and open to compromise. Media containing HMIS client identified data may not be shared with any person or agency other than the owner of the data for any reason not disclosed within the agency’s Privacy Notice.

HMIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

Software Application Security

Disaster Recovery

The Northern Illinois (NIL) HMIS Technical Lead Agency is responsible for ensuring that its vendors meet all regulated Disaster Protection and Recovery requirements. Currently the vendor commits itself to the following:

- Nightly database tape backups.
- Offsite storage of tape backups
- 7-day backup history stored locally on instantly accessible Raid 10 storage
- 1-month backup history stored off site
- 24 x 7 accesses to emergency line to provide assistance related to "outages" or "downtime".
- 24 hours backed up locally on instantly-accessible disk storage

Electronic Data Transmission

The NIL HMIS Technical Lead Agency is responsible for ensuring that its vendors meet all regulated Electronic Data Transmission requirements. Currently the vendor commits itself to the following:

- 128-bit SSL encryption is used to encrypt client data as it travels "over the wire" from the vendor's data center to the user's desktop.

Electronic Data Storage

The NIL HMIS Technical Lead Agency is responsible for ensuring that its vendors meet all regulated Electronic Data Storage requirements. Currently the vendor commits itself to the following:

- Data is stored in a binary format utilizing PostgreSQL data base application.
- Data is encrypted annually to provide an additional level of security.

Workstation Minimum Requirements

Any computer that interfaces with the HMIS must meet the minimum specifications or functionality cannot be guaranteed. Three main factors that can impact system performance are data transfer efficiency, memory management, and machine speed. Currently, the requirements are as follows:

Operating System

- Windows 7, 8, and 10

Memory

- 2GB RAM minimum, 4GB recommended

Monitor

- Screen Display - 1024 x 768 (XGA)

Processor

- Dual-Core processor

Internet Connection

Broadband

- Internet Browsers in order of compatibility: Google Chrome, Mozilla Firefox, Internet Explorer, Apple Safari.

There are additional requirements for the report creation functionality of the HMIS.

Computer Crime

Computer crimes violate state and federal law. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both. The System Administrator and users must comply with license agreements for copyrighted software and documentation. Licensed software must not be copied unless the license agreement specifically provides for it. Copyrighted software must not be loaded or used on systems for which it is not licensed. All users agree to this upon logging into the system for the first time and accepting the software's *End User License Agreement*.

Illinois Personal Information Protection Act

As discussed in **Section One** of this standard operating procedure, all agencies and users are bound to follow state and federal law and following those laws precede following this standard operating procedure. The steps outlined here are requirements of HMIS System Participation and should not be considered legal advice.

The Illinois Personal Information Protection Act (815 ILCS 530/5)[1] requires that data collectors who maintain Social Security numbers take sufficient measures to ensure the security of the data and to notify Illinois Residents if a data breach occurs. The collection of Social Security numbers is a mandatory requirement of HUD's minimum data collection requirements and thus both individual agencies as well as the HMIS are "Data Collectors" and are bound to the law. A client may be notified multiple times by each level of 'data holding' (HMIS Vendor, HMIS Lead, and individual agencies).

If a Breach Occurs at the Individual Agency

Upon detection of a breach of the security of the agency's data, the agency's Executive Director or Agency Data Administrator, must take the following actions:

1. Notification will be made to all Continuum of Care Contacts as listed on the HMIS website[2]
2. Notification will be made to individual agency clients in **one** of the following ways
   a. Written notice
   b. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in section 7001 of title 15 of the united states code[3]; or
   c. Substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds $500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following:
   (1) Email notice if the data collector has an email address for the subject persons;
   (2) Conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; **and**

(3) Notification to major statewide media

If Breach Occurs at a System Level

Upon detection of a breach of the security of the system data, the HMIS Lead must take the following actions:

1. Notification will be made to all Continuum of Care Contacts as listed on the HMIS website[2]
2. Notify each participating agency's Agency Data Administrator and Executive Director
3. The HMIS does not maintain adequate records for individual notification if a breach occurs (current address, phone number or email address). Provide a substitute notification by completing all of the following:
    a. Email Notice when an email address is available
    b. Conspicuous Posting to be added to the HMIS website
    c. Press Release to major statewide media

In either situation, the notice(s) must contain the following information:

1. The actual or approximate date of the security breach
2. The nature of the breach
3. A description of the steps that have or will be taken to address the breach
4. Toll-free number and address for each major consumer reporting agency (appendix xx)
5. Toll-free number, address and website for the Federal Trade Commission (appendix xx)
6. Include a statement informing the individual that they can obtain information from each of the consumer reporting agencies about fraud alerts and security freezes.

[1] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67

[2] http://www.dupageco.org/Community_Services/Community_Development/HMIS/35384/

[3] http://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap96-subchapI-sec7001.pdf