HMIS Privacy and Security

prepared by COHHIO

June 2020

HMIS Team

Genelle Denzin
HMIS Data Analyst

Matt Dicks
HMIS Technical Assistance and Training Support Coordinator

Amanda Wilson
HMIS Support Coordinator

Carolyn Hoffman
CoC Technical Assistance & Training Coordinator

Training Objectives

- Inform End Users of current HMIS privacy and security policy
- Prepare new End Users for obtaining their HMIS license
- Prepare existing End Users for HMIS Annual Renewal quiz

HMIS Background

HMIS from Concept to Implementation

- Data collection was done agency by agency in dBase, Excel, Access, homegrown systems
- HUD's purpose in defining an HMIS was to
  - Standardize data collection rules
  - Enforce uniform security methods
  - Reduce client duplication
- The first version of the HUD Data Standards was released in 2003
- The current version was released in 2019

Continuum of Care Level

Policy and Procedures Manual

- Reiterates HUD Standards and also clarifies COHHIO and DSA specific rules

Data Quality Standards

- Identifies reporting and performance requirements of HMIS program data

Client Data Protection

Personally Identifying Information (PII)

- Name, DOB, SSN, Race, Ethnicity, Gender

Additional Collected Data

- Disability status, history of homelessness, income, benefits, experience of domestic violence, services, referrals

Informed Consent

- Client preference
- Ability to refuse data collection

Client PII

Why do we collect Name/DOB/SSN?

- To uniquely identify clients and reduce duplicates

How is PII used/shared?

- PII data is only used for deduplication and coordination of services

Who has access to client PII?

- Case Managers, COHHIO HMIS Staff, WellSky tech support staff

Data Collection Rules

Posted Privacy Notice

- Required in a visible place at client intake

HMIS Data Privacy Notice & Consent

- Inferred consent only acceptable for SSVF and RHY clients
- Client can still refuse to provide data
- This may make client ineligible for certain services in certain programs

Data Collection Rules

Acknowledgment of Data Collection and Release of Information

- Client can still refuse to have certain information input into HMIS
- This may make client ineligible for certain services in certain programs

Informed Consent

Acknowledgment of Data Collection	Release of Information	HMIS Action
Client Accepts	Client Accepts	Enter client normally in HMIS.
Client Accepts	Client Declines	 Enter client and lock record.
Client Declines	Client Declines	 Enter client anonymously.

Don’t Know/Refused

Don’t Know

- All clients can respond *Don’t Know* if they can’t answer the question

Refused

- All clients can refuse to answer specific data elements. Refusal may impact eligibility for certain programs

Don’t know/refused data is considered missing for the purposes of state and federal reporting

Protecting Client PII

Handling client files

- Always keep secured from unauthorized eyes

Handling client data via email/fax/phone

- Fax of client PII may be appropriate between some agencies
- Do not email client PII
- Discussing client PII may be appropriate between certain agencies

Protecting Client PII (continued)

Computer Access

- Computer access needs to be private or supervised during data entry

Login Access

- Login access must be secured for only HMIS authorized users

No account sharing

- Login access shared between authorized users should never occur

Protecting Client PII (continued)

No client information leaving the building via contractors or visitors

- No information or data about clients being served should ever be taken out of the agency and shared in the community without client consent

Notify COHHIO when users leave or stop working with HMIS

- COHHIO must be notified when an HMIS user leaves and agency or ceases to work with HMIS. Access must be terminated immediately

Computer and Network Security

Mandatory

- Firewall
- Anti-virus software
- No password saving/ no auto-login

Optional

- Use Firefox or Chrome browser
- Anti-malware software

Computer Security

Do not write down HMIS passwords

- Not on monitor, not under keyboard, not in desk drawer

Computers in a publicly visible area must be monitored by Supervisor if used for HMIS

- Ideally a computer should be private and not be visible by passing foot traffic
- If not, data entry must be done while area is supervised

Computer Security

Web browser must not remember password or automatically log user into ServicePoint

- Do not use software like Wallet, Password Robot, and LastPass.
- Browser should stop at login to await user input

Logout when walking away from desk

Lock desktop with password screen-saver

- Set a screensaver to start after a few minutes on inactivity.
- Require a **password** to wake the computer from sleep or **screen saver.**

Annual Renewal

- Policies and Procedures for your CoC
  - Ohio Balance of State
  - Mahoning
- Data Quality Standards for your CoC
  - Ohio Balance of State
  - Mahoning
- HMIS Annual Renewal Quiz
- End User Agreement

Questions

email HMIS at
hmis@cohhio.org