# HMIS Privacy and Security

prepared by COHHIO
June 2017

## Introduction

- Purpose of training
  - Inform users of current HMIS Privacy and Security Policy
  - Prepare users for Security Quiz
  - Review standards for annual retesting

## HMIS Background

- HUD – HMIS from concept to implementation
  - Data Collection was already being done agency by agency in dBase, Excel, Access, homegrown systems
  - Standardize Data Collection Rules
  - Enforce Uniform Security Methods
  - Reduce Client Duplication

## HMIS Background

- Data Standards
  - 2003 HMIS Data Standards
  - 2004 VAWA Amendment
  - 2009 DSA VAWA Decision
  - 2010 HMIS Data Standards
  - 2014 HMIS Data Standards
  - 2015 Critical Updates
  - 2016 Critical Updates
  - 2017 HMIS Data Standards

## Ohio Balance of State

- Policy and Procedures Manual
  - Reiterate HUD Standards and also clarify COHHIO and DSA specific rules
- Data Quality Standards Manual
  - Identify Reporting and Performance requirements of HMIS Program Data

## Client Data Protection

- Personally Identifying Information
  - Name, DOB, SSN, Race, Ethnicity, Gender
- Additional Collected Data
  - Homeless Assessment; Income, Benefits, Services
- Informed Consent
  - Client preference
  - Ability to refuse data collection

## Client PII

- Why do we collect Name/DOB/SSN
  - To uniquely identify client and reduce duplicates
- How PII is used/shared
  - PII data is only used for deduplication and coordination of services
- Who has access
  - Case Managers, DSA Housing Staff, COHHIO HMIS Staff, Bowman Systems tech support staff

## Data Collection Rules

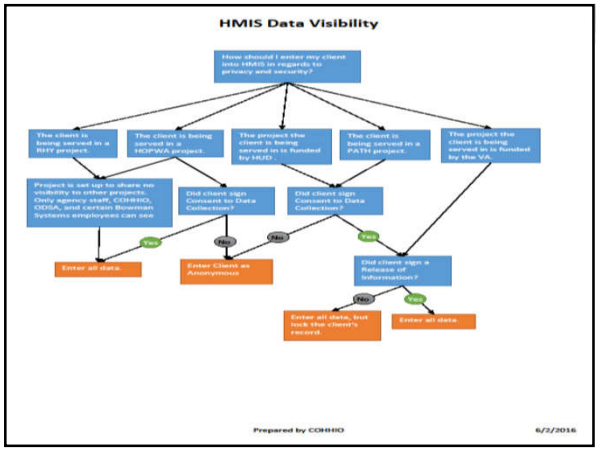
- Posted Notice
  - Required in a visible place at client intake
- HMIS Data Privacy Notice & Consent
  - Inferred consent only acceptable for SSVF and RHY clients
  - Client can still refuse to provide data
  - This may make client ineligible for certain services in certain programs

## Data Collection Rules (cont'd)

- HMIS 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

- Consent to data collection AND Release of Information
  - When both of these documents are signed, information is shared throughout the HMIS
  - The exception is HOPWA and RHY clients
- Consent to data collection ONLY
  - When only this document is signed, client record must be locked
- Client refuses to sign either form
  - Data is entered 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
  - Emailing of client PII is not appropriate
  - Discussing client PII may be appropriate between certain agencies
- 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

## Protecting Client PII

- No account sharing
  - Login access between authorized users should never occur
- No client information leaving the building via contractors, 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 / 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 password to HMIS
  - On monitor, under keyboard, in desk drawer
- Computer in a publicly visible area (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 Wallet or Password Robot software
  - Browser should stop at login to await user input

## Computer Security

- Logout when walking away from desk
- Lock desktop with password protected screen-saver

## Security Breach Protocol

- Can be viewed in full at http://hmis.cohhio.org/index.php?pg=kb.page&id=54
- Most common are sharing username & password and emailing PII
- Account will be inactivated until Security Breach Quiz is passed and Security Breach Acknowledgement Form submitted

## Questions

- Email hmis@cohhio.org