HMIS Privacy and Security

February 15, 2023

System Performance Committee

KCRHA
King County Regional Homelessness Authority

HMIS Consent Laws

- RCW 43.185C.180

1. Clients Must Opt - In
2. Must be provided Informed Consent
3. Must have Consent Documented

“**Personally identifying information about homeless individuals for the Washington homeless client management information system (HMIS) may only be collected after obtained informed, reasonably time limited** (i) written **consent** from the homeless individual to whom the information relates, or (II) telephonic consent from the homeless individual, provided that written consent is obtained at the first time the individual is physically present at an organization with access to the Washington homeless client management information system.”

What is Personally Identifiable Information?

Information which can be used to distinguish or trace an individual's identity, such as their name or social security number, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date of birth, etc.

<u>Information Provided About:</u>

- Name
- Date of Birth
- Social Security Number
- Other combinations of factors that could Identify someone

De-Identified Client Profiles

- If client declines consent
    - Clients can revoke consent at any time.
- HMIS users must follow protocol outlined in HMIS End User Manual
- Collect demographic info on gender, race, ethnicity and veteran status if possible
- Keep track of Unique Identifier
- Document “No” consent status behind Privacy Shield
- Discuss benefits of consent and identified data when client further engages, if appropriate

Partner Agency Privacy and Data Sharing Agreement (MOU)

Requirements of Partner Agencies include: (Full document here)

- No conditioning of services
  - Services cannot be withheld from clients based upon a client's refusal to have identified information in HMIS
- All HMIS users at every partner agency must complete HMIS confidentiality and ROI training
- Agency will not solicit from Clients or enter information about Clients into the HMIS database unless the information is required for a legitimate business purpose such as to provide services to the Client, to conduct program evaluation, to administer the program, or to comply with regulatory requirements.
- King County reserves the right to monitor and audit Partner Agency privacy practices to ensure compliance

Partner Agency Technical Administrator and Security Officer Agreement (TASO)

The Technical Administrator's responsibilities include: (Full Document here)

- Overseeing Partner Agency's Compliance with Data Sharing MOU
- Detecting and responding to violations of any applicable HMIS plans, forms, manuals, standards, agreements, policies, and governance documents
- Serving as the primary contact for all communication related to the HMIS at the Partner Agency and forwarding such information to all Partner Agency end users

Partner Agency Security Officer

Security Officer responsibilities include:

- Conducting a complete and accurate semi-annual review of the Partner Agency's compliance with all applicable plans, forms, manuals, standards, agreements, policies, and governance documents
- Completing the HMIS Semi-Annual Compliance Certification Checklist (the "Checklist"), and forwarding the Checklist to the HMIS System Administrator (Bitfocus)
- Continually monitoring and maintaining security of all staff workstations and devices used for HMIS data entry
- Investigating potential and actual breaches of either HMIS system security or client confidentiality and security policies, and immediately notifying the County and the System Administrator
- Developing and implementing procedures that will prevent unauthorized users from connecting to any private Partner Agency networks
- Ensuring all HMIS end users complete mandatory training before gaining HMIS access.

Unauthorized Access of Client PII

In cases of unauthorized access of client information, the Partner Agency must:

a. Immediately working to remedying or mitigating the issue that resulted in such unauthorized access;

b. Notifying KCRHA within 24 hours of any incident of unauthorized access to HMIS data, or any other breach in the Agency's security that materially affects County or HMIS;

c. Upon request from KCRHA, Agency shall provide a corrective action plan that addresses the incident and is designed to ensure compliance by its officers, employees, agents, and subcontractors with the confidentiality provisions in this Agreement; and

d. Agency will be responsible for notifying all impacted clients.

(This text is pulled from the Privacy and Data Sharing MOU)

Involuntary Removal of HMIS Users or Agencies

It is vital for the KCRHA and Bitfocus to provide a secure service for all Users. Any action(s) that threaten the integrity of the system will not be tolerated.

- Bitfocus reserves the right to modify, limit, or suspend any user account or remove any Partner Agency at any time if there is a security risk to the system.

- The penalties imposed on a user for improper system use will vary based on the level of the offense. Typically the user will receive a warning upon the first offense. However, if the offense is severe enough, Bitfocus reserves the right to disable the account immediately and, in extreme cases, to disable all users' access at the Partner Agency in question.

- If a user's account is suspended, only the Executive Director (or acting Executive Director) for a Partner Agency may request account re-activation. Suspended users may be required to attend additional training before having their access reinstated.

- In the event that a Partner Agency is removed from the system, it must submit a written request for reinstatement to KCRHA and Bitfocus.

(This text is pulled from the Privacy and Data Sharing MOU)

Other Privacy and Security Documents

King County HMIS Security Plan
Includes HUD rules for implementation of specified security standards. These security standards are designed to ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards; and ensure compliance with all applicable standards by end users.

King County HMIS Security Officer Compliance Certification Checklist
Checklist that is filled out by Security Officer semi-annually and sent to Bitfocus.

HMIS User Policy and Code of Ethics
This form must be completed upon HMIS users' initial login and every year thereafter.

HMIS Lead Improvement Evaluation Matrix

HUD publishes a list of questions for the CoC (in our case the SPC) to identify areas of improvement for the HMIS Lead (KCRHA). Questions relevant to HMIS Privacy and Security include:

✓ **Question 3.1 [System Administration]**: Does the HMIS Lead perform all system administration, management, and operational tasks in accordance with applicable MOUs, contracts, or statements of work?

✓ **Question 3.2 [System Administration]**:Has the HMIS Lead implemented project set up and data collection guidance per HUD and federal partner program HMIS Manuals?

✓ **Question 4.1 [Policy Implementation and Development]**: Does the HMIS Lead actively collaborate with the CoC to review, revise, and approve a privacy plan, security plan, and data quality for the HMIS?

HMIS Lead Improvement Evaluation Matrix

✓ **Question 4.2 [Policy Implementation and Development]**: Does the HMIS Lead actively support the CoC in the development and implementation of a data-sharing and consent framework that facilitates the sharing of client records based on applicable federal, state, and local statutes and the business needs (such as coordinated entry) of the CoC?

✓ **Question 4.3 [Policy Implementation and Development]:** Does the HMIS Lead actively manage data sharing settings by end users, programs, projects, and agencies to appropriately support datasharing in the HMIS implementation in accordance with the CoC's HMIS Privacy Plan?

✓ **Question 4.4 [Policy Implementation and Development]:** Does the HMIS Lead work collaboratively with the CoC to define data ownership policies both at the individual and household level as well as at the HMIS implementation level, to account for scenarios related to client revocation of consent or for HMIS software vendor change?

HMIS Lead Improvement Evaluation Matrix

✓ **Question 4.5 [Policy Implementation and Development]:** Does the HMIS Lead monitor HMIS-participating agencies and HMIS end users for electronic compliance with the CoC's HMIS security plan, such as user account management and password resets, system inactivity, internet browser security, firewall protections, and antivirus programs?

✓ **Question 4.6 [Policy Implementation and Development]:** Does the HMIS Lead monitor HMIS participating agencies and HMIS end users for physical compliance with the CoC's HMIS security plan, and is the monitoring process effective at decreasing security issues related to physical compliance?

✓ **Question 4.7 [Policy Implementation and Development]:** Does the HMIS Lead provide quality improvement strategies, training and capacity building opportunities, and corrective action planning to agencies and end users based on the findings of the HMIS end user monitoring process regarding privacy, security, and data quality?

HMIS Lead Improvement Evaluation Matrix

✓ **Question 4.11 [Policy Implementation and Development]:** Does the HMIS Lead have escalation protocols in place to inform leadership from HMIS participating agencies and the CoC when noncompliance with any HMIS privacy, security, or data quality plans is identified through the monitoring process?