How to Safeguard Clients' HMIS Data

Keeping data safe involves all parties. Below is information on how service providers collecting data can keep records safe and secure, as well as what data managers do to protect client information.

How do I keep client's data safe when accessing HMIS?

Prevent Unauthorized Viewing

- Avoid if possible conducting intakes or assessments in public areas
- Always use secure, agency-approved devices for data entry with VPN access
- Never leave confidential information in public view, such as on desks, photocopiers, fax
- When sharing screen, do not display client PII information (Personally Identifying Information)

Prevent Unauthorized Access

- Do not share passwords
- Each user must have a unique login and never share credentials
- HMIS access follows "least-privilege" principles—only access what is needed
- Do not store reports or other data on a shared computer and on shared drives
- Do not leave HMIS open and unattended, always log out of HMIS when stepping away from your workstation

When is sharing data outside of the HMIS safe?

Care coordination for the purposes of services to assist a client can be shared with other HMIS Partner Agencies to coordinate referral and placement for housing and services such as counseling, food, utility assistance and other services. There are strict legal guidelines for who has access to the information, and it is protected by electronic encryption.

Some important considerations;

- Make sure that you are sharing data with a known provider. If you don't know the person, ask for verification via email or other means before sharing information either over the phone or via electronic mail
- Only share what is most necessary for care coordination

REMINDER: All other data sharing is NOT permitted unless specifically requested by the client via additional release.

If anyone is pushing for access or information: Stop and talk with your supervisor, agency director or HMIS Lead at your agency.

Any external requests for HMIS data for any other reason (e.g., from government agencies or law enforcement) must be directed to KCRHA as the HMIS lead to review and respond.

How do I share information safely?

- Verify client consent before sharing
- Do not share PII outside of HMIS (Names, birthdates, SSNs, addresses, and any other unique identifiers)
- Do not email, text, or discuss client data unless using a secure, agency-approved method.

See something say something

- Be mindful of phishing attempts, unauthorized login attempts, and fake requests for HMIS access.
- If something seems suspicious, verify before responding.
- Work with your HMIS lead at your organization to assess any unusual activity and contact the KCRHA HMIS Lead Administrator if you need guidance on how to proceed.

Report Any Unauthorized Access or Data Breaches

- If you suspect unauthorized access to HMIS or an attempt to obtain client data improperly, immediately report it to:
    - Your Agency's Security Officer & HMIS Lead
    - KCRHA's HMIS Lead Administrator
    - The Bitfocus HMIS Support Team (kcsupport@bitfocus.com)
- Agencies must document all breaches and take corrective action to prevent future incidents.

These guidelines provide critical guidance on HMIS security, privacy protections, and data-sharing protocols, helping to protect client privacy, ensure data security, and maintain compliance with HMIS policies. If you have questions or need further clarification, contact your HMIS Administrator or the KCRHA HMIS Administrator at kcsupport@bitfocus.com or 206-444-4001 ext. 2.