Homeless System Response:

HMIS Security Basics

Introduction

As Continuums of Care (CoCs) are moving from individual program-by-program decision-making toward a community data-driven system response in ending homelessness, there is an increase in client data sharing amongst providers both inside and outside of the Homeless Management Information System (HMIS). The way that client data is accessed, shared, and stored is changing due to advancements in technology and evolving work environments caused by COVID-19. In response to these changes, communities must ensure that they continue to adhere to HMIS Security baseline standards from the 2004 HMIS Data and Technical Standards Final Notice as well as the recommendations and guidance from the Coordinated Entry Management and Data Guide.

Security Roles and Responsibilities

Data security refers to methods in which client data is protected from unconsented, intentional or accidental access by unauthorized parties. In the Coordinated Entry Notice, the United States Department of Housing and Urban Development (HUD) clarifies whether a CoC uses HMIS or "a system other than HMIS to record information from a coordinated entry process, it must meet HUD's requirements in 24 CFR 578.7(a)(8) and Section II.A and be compliant with HUD's HMIS Privacy and Security Notice." CoCs and providers each have a role and responsibility in securing and limiting access to each client's data. The following roles and responsibilities should be written into the CoC's policies and procedures:

CoC	The CoC is responsible for reviewing, revising, and approving the security plan for the HMIS implementation. The CoC must be familiar with the most recent baseline security standards written in HUD HMIS security regulations or notices. CoCs must ensure they are aware of updated guidance to address current needs and that they do not violate the 2004 baseline standards located in the COVID privacy documents and the Coordinated Entry Management and Data Guide.
HMIS Lead	The HMIS Lead must maintain data security by implementing the security plan, monitoring access to the system and processes for data handling, and training end users in security protocols. HMIS Leads should also work with their software vendor to ensure the hardware, software, and physical environments that store, transmit, and/or process data are compliant with HUD HMIS security baseline requirements. Additional roles and tasks for HMIS Leads are explained in the HMIS System Administrator Checklist.
Covered Homeless Organization	A covered homeless organization (CHO) is defined as any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, or processes data on clients experiencing homelessness for an HMIS. Although HMIS Leads are responsible for maintaining the security in the HMIS, they cannot prevent all breaches due to external data usage. CHOs, as entities that collect and enter data into the HMIS, need to understand that security breaches can happen outside of HMIS, and need to be aware of and implement the security plan to prevent potential external breaches. Data collected from clients is sensitive and includes personal information about their health, trauma, and experience of homelessness. As soon as the information is received from a client, CHOs become responsible for the security of that information.

Client information that is disclosed outside of a secure electronic HMIS is more susceptible to security breaches, which is why CHOs should pay attention to how they are handling and sharing data, so they are not allowing unauthorized access to client information. As CHOs coordinate services and housing with other providers, they should ensure no personally identifiable information (PII) is disclosed through unsecured means such as cloud-based documents like Google Sheets, unsecured video conference calls, and email.

Overall Security

Physical	Physical security involves protecting the systems through physical means. Work and home offices or other locations where PII is collected and stored either electronically or in hard copy are required to have either lockable offices or file cabinets, etc. to store any PII when not in use. This data cannot be left unattended.
Personal	Personal security concerns the people with access to any PII data. There is no HUD requirement for background checks, but they are a common practice for positions with access to large amounts of PII. Background checks, however, have a long history of disproportionate negative impacts on Black, Indigenous, and other people of color. These checks are often fraught with errors, mismatched identities, and incomplete information, and the use of background checks should be considered only with the input of the community.
Organizational	Organizational security refers to a set of policies and procedures developed by both the community and organizations (such as End User Agreements) that are used to ensure that people are using the systems and data appropriately.

Data Security and System Security

- System security covers multiple parts of the systems, including the following:
  - Controlling access to the HMIS system through passwords.
    - All users must have their own unique username and are not allowed to share user account information with anyone. No one should ask for your password, including systems administrators.
    - Passwords are only effective if they are kept private, strong, and not easily guessed. Passwords should be eight characters at a minimum—though 12 characters is preferable—with a combination of uppercase and lowercase letters, numbers, punctuation, and special characters. Some examples users could implement are:
      - Creating a math formula such as “830-630=TwoHundred”
      - Using the same combination of keystrokes for a phrase or word, but adjusting the keystrokes on your keyboard up and to the right by one key. Example: “New York Central Park” would become “J43 &05o F4j65wp _w5o”
    - All workstations and servers must have a password to access the computer, along with a password-protected screen saver.

        - HMIS leads can consider two-factor authentication as an extra layer of security so the chance of a security breach is unlikely even if a password is stolen.
    - Controlling access to the HMIS system by limiting access. A user must not be allowed to access the HMIS system from multiple workstations at the same time.
    - Encryption/Transmission
        - All HMIS data that is transmitted electronically must be encrypted with at least 128-bit encryption and use either a secure socket layer (SSL) or a virtual private network (VPN). All files that contain PII including but not limited to HUD and Supportive Services for Veteran Families (SSVF) comma-separated value (CSV) files, Excel worksheets, and files used for external reporting must be encrypted prior to transmission. Please remember email is NOT a secure method of transmission unless the files are properly encrypted before sending.
            - Video meetings and conference calls in which PII is discussed must use a password to prevent unauthorized callers from attending the discussions.
        - Backup and Disaster Recovery
            - HMIS data must be backed up regularly and stored offsite from the servers.
                - Virus Protection/Firewalls
                    - All workstations accessing HMIS (including remote and VPN users) must have regularly updated anti-virus software that scans files periodically.
                    - All servers, workstations, and networks must have either a hardware or software firewall that is updated regularly.
                - Secure Disposal
                    - All electronic devices used to access HMIS data must be disposed of properly to ensure data has been completely erased from the devices. All hard copy reports containing PII data must also be destroyed (i.e., shredded) when no longer needed.
                - Physical Access/Location
                    - Access to workstations must be controlled and monitored (i.e., locked offices, privacy screens, etc.). Servers must be controlled to a greater degree and be locked in a secure location.
                - Remote or Cloud Data Storage
                    - There are many cloud or offsite storage solutions available, and their usage is increasing. Some examples include Google Drive/Docs, DropBox, Microsoft 365, One Drive, etc. The same protocol must be used to vet remote or cloud storage solutions for their encryption and storage policies as would be done with any HMIS vendor where data is stored on remote servers.
                - Smartphones/Tablets
                    - With the increased use of smartphones and tablets in the field, the same protocol must be followed as with local workstations. These devices must be password protected and stored in secure locations when not in use.
                    - Enable remote erase and location functions on these devices in the event they are lost or stolen.
- Hard copy security involves the protection of hard copy data that contains any PII.
    - Hard copies, paper forms, or reports that contain any PII must be supervised while in a public area and stored in a secure location when not in use.

- By-name lists or other documents used during meetings that contain PII must be accounted for and properly stored or destroyed when finished. Do not put reports that contain PII in the garbage or recycle bin in a meeting area; these should be shredded.

Conclusion

As communities work toward maintaining and improving data security measures, CoCs need to prepare for the possibility of a security breach and how to manage a breach if it occurs. HUD does not provide guidance on how a community responds to a breach, but it does state that a CoC must have a process for handling a breach. There should be a legal review of state, local, and other federal privacy laws to determine if there are more restrictive or limiting requirements for data in HMIS. If so, these laws will need to be considered when developing your local HMIS data collection and security policies.