

4. Standards for Data Confidentiality and Security

This section describes standards for the security of data collected and stored in HMIS at a local program or at a central storage facility, and the rights of individuals who are participating in the HMIS to have personal information kept secure. The intent of this section is to ensure the privacy and confidentiality of information collected by HMIS, while allowing for the use of data as needed by homeless assistance programs, CoCs and researchers. The information contained in this section of the notice is based upon common practice and standards within the information technology community, as well as in large measure upon the HIPAA (Health Insurance Portability and Accountability Act of 1996) standards for securing and protecting private medical information.

This section describes the minimum standards required by federal law. State and local laws may require confidentiality and security standards beyond those described in this notice. Local CoCs may also develop additional protocols or policies to further ensure the privacy and confidentiality of information collected through HMIS.

4.1 Protected Personal Information

This section identifies specific types of information that are considered protected personal information.

Any information that can be used to identify a particular individual is protected personal information. An HMIS user for these purposes is defined as program staff (or trained volunteers) and CoC system administrators who use the HMIS. A developer is defined for these purposes as both the individuals and organization responsible for developing the HMIS and any functionality that is built into HMIS. HMIS users and developers should consider the following to be protected personal information of an individual and his or her relatives, employers, or household members:

- Names.
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes.
- All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, and date of death.
- Telephone numbers.
- Social Security numbers.
- Medical record numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.

- Device identifiers and serial numbers.

- Any other unique identifying number, characteristic, or code.

The HMIS user or developer must not use any other data element to identify an individual. Any other data element that can be used to identify an individual is considered protected personal information.

4.2 Securing HMIS and Data

This section describes the standards for system and application security.

System Security

Applicability. These system security provisions apply to the systems where the HMIS application is installed (networks, desktops, laptops, mini-computers, mainframes and servers).

User authentication. HMIS workstations and server shall be secured with, at a minimum, a user authentication system consisting of a username and a password. Passwords shall be at least eight characters long and meet industry standard complexity requirements, including, but not limited to, the use of at least one of each of the following kinds of characters in the passwords: Upper and lower-case letters, and numbers and symbols. Passwords shall not be, or include, the username, the HMIS name, or the HMIS vendor's name. In addition, passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards. The use of default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use.

Written information specifically pertaining to user access (e.g., username and password) shall not be stored or displayed in any publicly accessible location.

Virus protection. HMIS workstations and server shall be protected from viruses by commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed.

Firewalls. HMIS workstations and server shall be protected from malicious intrusion behind a secure firewall.

Public access. HMIS data shall not be housed on computers with public access to any part of the computer through the Internet, modems, bulletin boards, public kiosks, or similar arenas. HMIS that use such public forums for data collection or reporting must be secured to allow only connections from previously approved computers and

systems through Public Key Infrastructure (PKI) certificates, extranets that limit access based on the Internet Provider (IP) address, or similar means. Further information on these tools can be found in the HMIS Consumer Guide and the HMIS Implementation Guide, both available on HUD's website.

Physical Access to Systems With Access to HMIS Data

Computers that are used to collect and store HMIS data shall be staffed at all times when in public areas. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not publicly accessible. These steps should minimally include: Logging off the data entry system, shutting down the computer, and storing the computer and data in a locked room.

Disaster Protection and Recovery

HMIS data shall be copied on a regular basis to another medium (e.g., tape) and stored in a secure off site location where these same standards would apply. Ideally, off site storage shall include fire and water protection for the storage medium.

HMIS that store data in a central server, mini-computer, or mainframe shall store the central hardware in a secure room with appropriate temperature control and fire suppression systems.

Surge suppressors shall protect physical systems for collecting and storing the HMIS data.

Application Security

Applicability. These application security provisions apply to how the data are secured by the HMIS application itself, during entry, storage and review, or any other HMIS function.

User authentication. HMIS workstations and server shall be secured with, at a minimum, a user authentication system consisting of a username and a password. Passwords shall be at least eight characters long and meet industry standard complexity requirements, including, but not limited to, the use of at least one of each of the following kinds of characters in the passwords: Upper and lower-case letters, and numbers and symbols. Passwords shall not be, or include, the username, the HMIS name, or the HMIS vendor's name. In addition, passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards. The use of default passwords on initial entry into the HMIS application is allowed so