

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.

Electronic data transmission. MIS data that are electronically transmitted over publicly accessible networks or phone lines shall be encrypted to at least 128-bit encryption. Unencrypted data may be transmitted over secure direct connections between the two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data.

Electronic data storage. HMIS data shall be stored in a binary, not text, format. Protected personal information shall be stored in an encrypted format using at least a 128-bit key. This encryption must be done within the HMIS so that the data are not readable from outside the local HMIS application.

Hard Copy Security

Applicability. This section is intended to provide standards for securing any hard copy that is either generated by or for HMIS, such as reports, data entry forms, and signed consents.

Any paper or other hard copy generated by or for HMIS that contain individually identifiable information as defined in this standard must be under constant supervision by an HMIS user or developer when in a public area. When staff are not present, the information shall be secured in areas that are not publicly accessible.

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

4.3 Privacy of Protected Personal Information

An HMIS user or developer may not use or disclose protected personal information except to the individual whose information it is or as permitted or required by this standard or by law.

Uses and Disclosures of Protected Personal Information Assumed by Entry Into the HMIS

By providing data to HMIS user or developer for entry into HMIS, an individual provides oral assent to the uses described in the following section. Such assent should only be assumed if the individual has been advised how he

or she could benefit by providing the requested information, how the data will be protected, and how the data will be used.

An HMIS user or developer may use or disclose protected personal information without the written consent of the individual in situations specified in this notice, subject to the notice's applicable requirements. When the HMIS user or developer is required to inform the individual of, or when the individual may agree to a permitted use or disclosure, oral announcement is sufficient.

Uses and disclosures for administrative purposes. A CoC system administrator or developer may use or disclose protected personal information to program staff within the same program so they may perform necessary administrative functions (e.g., ensure data integrity and create an unduplicated count of homeless persons). For the purpose of creating an unduplicated count within a CoC in which data are accessible across programs, the CoC may decide that oral consent is not sufficient. This notice neither requires nor prohibits the sharing of client information among programs in the CoC, but does require that local policy regarding information sharing be established and that either client notification or written consent be provided for in the event that information is shared.

Uses and disclosures for academic research purposes. An HMIS user or developer may use or disclose protected personal information to individuals performing academic research who have a formal relationship with a local program or CoC. Such research would be conducted either by an individual employed by the program, so long as the research has been approved by a program administrator, or by an outside institution that has entered into a research agreement with the program or CoC. Such data are to be used within the boundaries set by an approved research agreement. Such approvals do not substitute for Institutional Review Board (IRB) approvals, and researchers should seek appropriate IRB approvals.

Use for creating de-identified information. An HMIS user or developer may use protected personal information to create information that is not individually identifiable or disclose protected personal information to a third party to be used only for such purpose, whether or not the de-identified information is to be used by the HMIS user or developer.

Uses and disclosures required by law. An HMIS user or developer may use or disclose protected personal information

to the extent that law requires such use or disclosure and the use or disclosure complies with and is limited to the relevant requirements of such law.

Disclosures about victims of abuse, neglect, or domestic violence. Consistent with applicable law and standards of ethical conduct, an HMIS user or developer may disclose protected personal information about an individual who is reasonably believed to be a victim of abuse, neglect, or domestic violence to a government authority (including a social service or protective services agency) authorized by law to receive reports of such abuse, neglect, or domestic violence. Disclosures to other entities are permissible only if the individual agrees to such disclosure.

Uses and disclosures to avert a serious threat to health or safety. An HMIS user or developer may, consistent with applicable law and standards of ethical conduct, use or disclose protected personal information if the HMIS user or developer, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

Uses and disclosures about decedents.

- Coroners and medical examiners. An HMIS user or developer may disclose protected personal information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

- Funeral directors. An HMIS user or developer may disclose protected personal information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to a decedent. If necessary for funeral directors to carry out their duties, the HMIS user or developer may disclose the protected personal information prior to, and in reasonable anticipation of, the individual's death.

Disclosures for law enforcement purposes. An HMIS user or developer may, consistent with applicable law and standards of ethical conduct, disclose protected personal information for a law enforcement purpose to a law enforcement official. Such disclosure should meet only the minimum standards necessary for the law enforcement official's immediate purpose and not disclose information about other individuals within the program or CoC not specifically required by that purpose. A court order or search warrant may be required for