Clear Form

Utah Homelessness Management Information System (Utah HMIS)
Data Security Monitoring Guide

AGENCY_____

CONTACT PERSONS /TITLES/CONTACT INFORMATION

_____

Utah HMIS Monitor_____

Date of Monitoring_____

A.	**Agreements and Authorization**	**Y, N, N/A**	**Comments**
1.	The agency has completed a UHMIS Agency Agreement and has provided a copy to the Utah HMIS.		
2.	The agency has completed a Utah HMIS End User Agreement for each authorized system user and has provided a copy to the Utah HMIS.		
3.	Is there a list of active authorized/certified HMIS users? (All staff entering/viewing HMIS data in the HMIS system must be appropriately trained and have and individual user license with a unique user name and password.)		
4.	The agency has reviewed the policies and procedures manual (August 2015 Version)		
B.	**Data Protection**	**Y, N, N/A**	**Comments**
1.	The agency collects, enters and extracts only HMIS data that are relevant to the delivery of homeless services		
2.	The agency limits access to the Utah HMIS database to its own employees specifically for: a. verifying eligibility for service b. entering records into the system for service provided.		

3.	As staff members leave the employ of the agency, their HMIS user accounts are immediately inactivated or changes to accommodate a new user. The agency must contact the Utah HMIS System Administrator to make these changes. (Written Procedures in place for turnover)		
4.	Is the UHMIS privacy policy posted in a common area viewable by those receiving services?		
5.	Signed "Client Consent for Data Collection" and "Client Consent for Data Release" forms from clients are kept on file. (The agency has a Quality Assurance Plan in place and monthly process that verifies that consents were obtained)		
6.	Data extracted from the database is stored in a secure location within the local area network. If data is transmitted outside of the local area network, it is properly protected via encryption or by adding a file-level password.		
7.	Do computers used to access the HMIS have a locking screen saver? (Terminals that access the HMIS system must have locking screen savers and are password protected. Terminals must be locked when left unattended.)		
8.	Terminals that access the HMIS system must have virus protection with automatic updates and individual or network firewalls.		
C.	**HMIS Best Practices**	**Y, N, N/A**	**Comments**
1.	How often is client information entered into HMIS? How is this documented? The agency accurately enters all the required HMIS data elements, as specified in the Agency Agreement, within 5 working days		
2.	Entry and Exit Dates are accurately reflected in HMIS (The agency has a Quality Assurance Plan in place and a process for verifying that entry and exit dates in administrative files match HMIS)		
3.	Do HMIS users have access to adequate computer technology and tools, such as internet access, printers, data analysis software, etc.?		
4.	Any other technical assistance?		