City of Cambridge
Homeless Management Information System (HMIS)

SECURITY PLAN

City of Cambridge Department of Human Service Programs
Planning & Development Division
51 Inman Street, 2nd Floor
Cambridge, MA 02139

Bitfocus, Inc. is the host of Clarity Human Services Software which operates Cambridge HMIS.Each partner agency is responsible for providing and maintaining computer hardware and Internet service. Each administrative staff or end user that a participating agency determines will have access to Clarity HMIS will be issued a user license (login ID and password) after the successful completion of HMIS Privacy and Security training and HMIS Beginner User training with accompanying signature of the CHMIS Partner Agency User Policy and Responsibility Agreement.

End User Accounts

CHMIS Project Staff will provide an End User Account username and initial password to each authorized End User once the HMIS beginner training has been completed and the CHMIS Partner Agency User Agreement Form has been signed. End User Accounts are assigned on a per-person basis, rather than to a particular position or role. End User Accounts are not to be exchanged, shared, or transferred between personnel at any time. Sharing of End User Accounts is a breach of these Policies and Procedures and a violation of the Partner Agency Agreement and the Partner Agency User Agreement Form.

Under no circumstances shall a Partner Agency demand that an End User hand over his or her username and password. The Partner Agency shall inform the CHMIS administrator of any changes in personnel or other requests to revoke or transfer accounts.

Licenses and access to Clarity HMIS will be disabled immediately for any staff that terminates employment or changes roles where Clarity HMIS access is no longer required. The Participant's Agency Administrator will notify the CHMIS System Administrators of staff changes within seven (7) business days.

End User Inactivity

End Users who have not logged into the system in the previous 90 days will be flagged as inactive. Inactive End Users will have their CHMIS accounts locked to maintain the security, confidentiality, and integrity of the system.

User Access Levels

The Partner Agency shall designate one User to be the Site Manager, identify and approve their respective users, and determine Clarity HMIS user access level for their respective users. The level will be based on each user's job function as it relates the Clarity HMIS's data entry and retrieval schema. HMIS Project Staff will aid in the determination of HMIS User access level when requested.

Passwords

End User Account passwords should never be written on any item left in their office, desk, or other workspace, and passwords should never be in view of any other person. Users will be forced to change their passwords every 180 days for security purposes.

Connectivity and Computer Systems

Partner Agencies will connect to CHMIS independently via the internet and are responsible for providing their own internet connectivity and computer systems sufficient for doing so. HMIS Project Staff provides technical support to Partner Agency's solely for CHMIS.

Workstation Security

At a minimum, the primary workstation used by each End User to log in to CHMIS should be configured to meet the following best practices:

- Password-protected log on for the workstation itself;
- Password-protected (aka locked) screensaver after five minutes or more of inactivity;
- Operating system updated with manufacturer's latest patches at least weekly;
- Ports firewalled;
- Systems scanned at least weekly for viruses and malware

HMIS Project Staff may provide some recommendations or advise in pursuing these best practices, but proper workstation configuration remains the responsibility of each Partner Agency.

Local Data Storage and Transfer

Partner Agency Users are responsible for maintaining the security and confidentiality of any client-level data extracted from the database and stored locally, including all data used in internal reporting. No identifiable client-level data is to be transmitted unless it is properly protected. Security questions should be addressed to CHMIS Project Staff.

Remote System Access

Partner Agencies and End Users must abide by these Policies and Procedures and ensure the security and confidentiality of client data regardless of the computer used to log in to the system. For this reason, End Users are strongly cautioned against extracting and storing personally identifiable client information on their personal computers and internet devices.

Client Access to Records

Clients may not be denied access to their own records. Clients have the right to see their information contained in CHMIS. If a Client requests, the agency staff must review the information with the client.

Training

HMIS Project Staff will coordinate adequate and timely training for all End Users prior to issuing an End User Account. Additionally, HMIS Project Staff provides training aids, reference material, and other support on the HMIS section of the Cambridge Continuum of Care website (http://cambridgecoc.org/hmis/training-guides-and-manuals/) and publishes HMIS News on a regular basis.

Annual Security Review

Cambridge Department of Human Service Programs Grant Managers shall conduct a review of physical and technical safeguards set forth in this plan during their annual program site visits.