Volusia/Flagler County Coalition for the Homeless
Homeless Management Information System

SECURITY PLAN

Background

This plan describes the plan for implementation of security policies and procedures for the Homeless Management Information System (HMIS) that is maintained by the Volusia-Flagler County Coalition for the Homeless, as the HMIS Lead Agency designated by Daytona/Deltona/Volusia-Flagler Counties FL-504 Continuum of Care (the CoC).

The Department of Housing and Urban Development (HUD) has mandated implementation of HMIS security standards and the creation of an HMIS Security Plan, as specified in the HMIS Interim Rule. The Plan must cover the Contributing HMIS Organizations (CHOs) as well as the HMIS Lead. It must ensure the confidentiality, integrity, and availability of all HMIS information; protect against reasonably anticipated threats or hazards to security; and ensure end user compliance. In addition, written policies and procedures must comply with all applicable Federal law and regulations and applicable state or local governmental requirements.

The Security Plan will be fully implemented following CoC approval and no later than 6 months after the finalization of the HMIS Interim Rule. In addition, the Security Plan will be reviewed and updated annually by the HMIS System Administrator in consultation with the HMIS Committee.

Outline

The Security Plan covers the following areas, some of which share overlapping concerns:

Administrative Safeguards:

1. Responsibilities of the HMIS System Administrator/HMIS Lead Security Officer
2. Responsibilities of the HMIS Site Technical Administrator/CHO Security Officer
3. Responsibilities of HMIS User
4. User training
5. Annual Security Review
6. User IDs and passwords
7. Role-based access to the HMIS and separation of concerns
8. Workforce Security

Physical Safeguards:

1. Computers used to access the HMIS system
2. Disposal of paper or electronic records
3. Disaster Recovery
4. Virus Protection
5. Secure Connection and Data Encryption

Administrative Safeguards

1. Responsibilities the HMIS System Administrator

The HMIS System Administrator will also be the HMIS lead security officer. The responsibilities of the HMIS lead security officer will be to:

a. provide annual training and guidance to CHO HMIS Site Technical Administrators and/or security officers.
b. develop, implement the Security Plan, and review it annually.
c. maintain contact information for the HMIS Site Technical Administrators and security officers of the CHOs.
d. be the primary contact for the CHO to report and resolve security issues.

2. Responsibilities of the HMIS Site Technical Administrator

The HMIS Site Technical Administrator for each CHO will designate a CHO Security Officer, who will frequently also be the same person as the Site Technical Administrator. The responsibilities of the CHO Security Officer will be to:

a. provide contact information for the CHO Security Officer to the Lead HMIS Security Officer.
b. ensure all new CHO HMIS Users receive security training before using the HMIS System.
c. ensure all CHO HMIS Users receive an annual refresh to their security training.
d. maintain a list of active HMIS Users.
e. notify the HMIS lead security officer within 24 hours when an HMIS User no longer requires HMIS access so the User account can be deactivated.
f. ensure the CHO and all HMIS Users comply with the security policies specified in the HMIS Policies and Procedures.

3. Responsibilities of the HMIS User:

a. Undergo HMIS training before use of the HMIS System and an annual security training follow up, as prescribed by the HMIS Lead Security Officer.
b. Comply with the security policies specified in the HMIS Policies and Procedures.
c. Report any incident in which unauthorized use or disclosure of personally identifying information (PII) has occurred and any incident in which PII may have been used in a manner inconsistent with the HMIS Policies and Procedures.

4. User training:

HMIS Users will be given security training before gaining access to the HMIS. Refer to Policies and Procedures "Section 3: Training" for a description of the topics covered.

5. **Annual Security Review:**

   The HMIS Lead Security Officer and each CHO will perform a yearly on-site security review of the CHO to ensure compliance with the Security Plan. The HMIS Lead Security Officer will prescribe any steps needed to bring the CHO into compliance. The CHO will follow these audit recommendations to the best of its ability.

6. **User IDs and Passwords:**

   Access to the HMIS System is controlled via a User ID and password. The CHO Security Officer will assign User IDs and a one-time password to new HMIS Users. See HMIS Policies and Procedures Section 2: Participation Requirements, "User Accounts" for a full description of the protocol for assigning User IDs and selecting and maintaining passwords, which must be changed every 45 days.

7. **Role-based access to the HMIS and separation of concerns:**

   Authorization of application functions in modern software like the HMIS System is typically role-based. The permission to perform an application function is granted to a role, (for example "system operator" or "resource specialist") rather than directly to a user. Then, users are assigned the role(s) necessary to perform their required tasks. (See HMIS Policies and Procedures Section 2: "Information Security Protocols, 8. Access Levels" for a fuller description of this process, along with examples.) An appropriate separation of concerns is enforced by assigning a user the correct roles and removing them when they are no longer needed. The HMIS Lead Security Officer will periodically review the role definition, role assignment, and authorization decisions of each CHO and prescribe changes as necessary.

8. **Workforce Security:**

   The CHO will perform a background check on its designated Security Officer and on any administrative users of the HMIS System.

Physical Safeguards

1. **Computers used to access the HMIS system:**

   Physical access to any computing device used to access the HMIS System must be controlled and limited. A CHO will ensure that computers stationed in public areas used to collect and store HMIS data are staffed at all times. All workstations will be required to have password-protected screensavers that are activated within 5 minutes of inactivity. When a computing device used to access the HMIS System is going to be unattended

for more than 15 minutes, the HMIS User will log out of the HMIS System and shut down or otherwise disable the device.

2. **Disposal of paper or electronic records:**

   The CHO will dispose of documents that contain PII by shredding paper records, deleting any information from magnetic media before disposal, and deleting any copies of client-level data from any device before transfer or disposal of the device. The HMIS System Administrator will assist if necessary in disposing of any electronic client-level data.

3. **Disaster Recovery:**

   The CoC's HMIS data is stored by the HMIS Vendor (ServicePoint™) in an off-site location, with backup, in encrypted form. In the event of disaster, the HMIS System Administrator will coordinate with the HMIS Vendor to ensure the HMIS System is restored. Following recovery, the HMIS System Administrator will be the point of contact to communicate to CHOs when the HMIS System becomes accessible.

4. **Virus Protection:**

   A CHO will protect computing devices used to access the HMIS System by installing virus protection software. Virus protection will include automated scanning of files as they are accessed, and virus definitions will be updated at least weekly.

5. **Secure Connection and Data Encryption:**

   All network communication with the HMIS System will be sent over a secure connection. All copies of HMIS data containing PII will be made in encrypted form.