Homeless Services Network of Central Florida

Homeless Management Information System

Policy Handbook

May 2016

Introduction

Homeless Services Network of Central Florida (HSN) is the lead agency for the Continuum of Care in Central Florida. The Continuum of Care is the community's strategic plan for the organization and delivery of services to people who are homeless in Orange, Seminole, and Osceola Counties. The result of the Continuum of Care process is a coordinated, multi-agency system of the services ranging from outreach to permanent housing, which address many of the housing and supportive services needs of both homeless individuals and families in Central Florida.

HSN has implemented a Homeless Management Information System (HSN HMIS) to facilitate the collection of information on homeless individuals and families throughout the Continuum of Care. HMIS data can be employed to better understand the characteristics of homeless persons in the community, improve the delivery of housing and services homeless persons, and document the community's progress in reducing homelessness.

HSN recognizes the importance of maintaining confidential client records in a secure environment to insure that the information is not misused or accessed by unauthorized people. The following Policies and Procedures have been developed to establish standards for the collection, storage and dissemination of confidential information by the users of the HSN-HMIS.

Governing Principles

Described below are the overall governing principles upon which all other decisions pertaining to the HSN-HMIS project are based.

The HSN-HMIS will be:

- A confidential and secure environment for the collection and use of client data.
- A benefit to individual clients through enhanced service delivery.
- A tool for the provider Agencies in managing programs and services.
- A guide for HSN and its funders through compilation of aggregate data regarding community resource needs and service delivery.

HMIS Benefits

Benefits for service providers

- Provides online real-time information about client needs and the services available for homeless persons.
- Assures confidentiality by providing information in a secured system.
- Decreases duplicative client intakes and assessments.
- Tracks client outcomes and provides a client history.
- Generates data reports for local use and for state and federal reporting requirements.
- Facilitates the coordination of services within an organization and with other agencies and programs.
- Provides access to a regional database of service providers, allowing agency staff to easily select a referral agency.

Benefits for homeless persons

- Intake information and needs assessments are maintained historically, reducing the number of times homeless persons must repeat their stories to multiple service providers.
- The opportunity to provide intake and life history one time demonstrates that service providers consider the homeless person's time is valuable and restores some of the consumer's dignity.
- Multiple services can be easily coordinated and referrals streamlined.

Benefits for policy makers

- Better able to define and understand the extent of homelessness throughout the region.
- Better able to focus staff and financial resources to the agencies and programs in geographical areas where services for homeless persons are needed the most.
- Better able to evaluate the effectiveness of specific interventions and specific programs and services provided.
- Better able to provide the State Legislature and the federal government with data and information on the homeless population in Central Florida.
- Better able to meet all federal reporting requirements.

HMIS Roles And Responsibilities

HMIS Lead Agency

1. Implement and continuously improve HSN's HMIS.
2. Ensure the HMIS scope aligns with the requirements of agencies, HUD and other stakeholder groups.
3. Address any issue that has major implications for the HMIS, such as policy mandates from HUD or performance problems with the HMIS vendor.
4. Reconcile differences in opinions and approaches, and resolve disputes arising from them.
5. Review, revise and approve HMIS policies developed by the HMIS Program Manager.
6. With the FL 507 Continuum of Care Board of Directors develop and approve the HMIS Policies and Procedures as the governance charter.

HMIS Software Vendor

1. Design the HMIS to meet HUD HMIS Data Standards.
2. Provide ongoing support to the HMIS Program Manager pertaining to needs of end-users to mine the database, generate reports and other end-user interface needs.
3. Administer the product servers including web and database servers.
4. Monitor functionality, speed and database backup procedures.
5. Provide backup and recovery of internal and external networks.
6. Maintain the system twenty-four hours a day, seven days a week.
7. Communicate any planned or unplanned interruption of service to the HMIS Program Manager.

HMIS Program Manager

1. Oversee all contractual agreements with funders, participating organizations and consultants in adherence to the policies and practices of HMIS and recommendations of the HMIS Steering Committee.
2. Monitor compliance with HUD's HMIS standards and guidelines and periodically review control decisions.
3. Provide training to participating organization leadership and other stakeholders regarding HMIS policies and procedures.

4. Authorize usage and access to HMIS for users who need access to the system for technical administration, data entry, editing of client records, viewing of client records, report writing, or administration of essential activities associated with carrying out HMIS responsibilities.
5. Develop reports.
6. Mine the database to respond to the information needs of participating organizations, community stakeholders and consumers by providing support through the help desk. http://support.hsncfl.org
7. Document work on the database and the development of reports/queries.
8. Provide technical assistance as needed with program sites.
9. Provide training and technical assistance to participating organizations on policies and procedures and system use.
10. Respond to questions from user via the HMIS helpdesk tickets.
11. Coordinate technical support for system software.
12. Communicate problems with data entry and support data quality to participants.
13. Monitor agency participation including timeliness and completeness of entry.
14. Communicate any planned or unplanned interruption in service.
15. Audit policy and procedure compliance.
16. Serve as the applicant to HUD for any HMIS grants that will cover the Continuum of Care geographic area.
17. Complete an annual security review.

<u>HMIS Support Specialist</u>

1. Edit and update agency information in HMIS.
2. Ensure that the participating agency obtains a unique user license for each user at the agency.
3. Ensure a minimum standard of data quality by answering all the HUD Universal Data Elements for every individual entered into HMIS by the agency.
4. Maintain the HUD required elements for each program.
5. Train new staff persons on HMIS, including reviewing the policies and procedures and any agency policies that impact the security and integrity of client information.
6. Ensure that HMIS access is granted only to staff members that have received training

and are authorized to use HMIS.

7. Grant technical access to HMIS for persons authorized by the HMIS Program Manager by creating usernames and passwords.
8. Notify all users at their agency of interruptions in service.
9. Provide a single point of communication between users and HMIS staff
10. Administer and monitor data security policies and standards, including:
11. User access control
12. Back and recovery of data
13. Detecting and responding to violations of HMIS Policies and Procedures

HMIS User

1. Take appropriate measures to prevent unauthorized data disclosure.
2. Report any security violations.
3. Comply with relevant policies and procedures.
4. Input required data field in a timely manner.
5. Inform clients about agency use of HMIS and relevant privacy policies.
6. Take responsibility for any actions undertaken with his or her username and/or password.

HMIS Administration Requirements

Participation Agreement Documents

Partner Agencies must complete the following documents:

- HMIS Partner Agency Agreement must be signed by each participating agency's executive director. The participation agreement states the agency's commitment to adhere to the policies and procedures for effective use of HMIS.
- HMIS User Agreement must be signed by each authorized user.

HSN will retain the original, signed documents.

User Access to the System

The participating homeless serving agency will work with HMIS staff to determine the appropriate user access level for all staff who will be granted access to HMIS. All HMIS users

must receive training before access to the system is granted. The HMIS Support Specialist will generate username and passwords within the administrative function of the software.

Passwords

- Creation: Passwords are automatically generated from the system when a user is created. The HMIS Support Specialist will communicate the temporary, system-generated password directly to the user.
- Use: The user will be required to change the password the first time they log onto the system. The password must be at least 8 characters and include two numbers or symbols. Passwords should not be able to be easily guessed or found in a dictionary. Passwords are each user's responsibility and users cannot share passwords. Users may not keep written copies of their password in a publicly accessible location.
- Storage: Any passwords that are written down are to be stored securely and must be inaccessible to other persons. Users are not to store passwords on a personal computer for convenience.
- Expiration: Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until 2 password selections have expired.
- Unsuccessful logon: If a user unsuccessfully attempts to log-on 3 times, the User ID will be "locked out," and the user account will be de-activated, rendering the user unable to gain access until his/her password is reset by HMIS staff.

Inputting Data

Agencies participating in the HMIS must meet the minimum data entry requirements established by the HUD Standards. Program entry and exit dates should be recorded upon any program entry or exit on all participants. Entry dates should record the first day of service or program entry with a new program entry date for each period/episode of service. Exit dates should record the last day of residence in a program's housing before the participant leaves the shelter or the last day a service was provided.

Tracking of Unauthorized Access

Any suspicion of unauthorized activity should be reported to HMIS staff.

Agency HMIS Administrators

Agencies will be required to assign one person to be an Agency HMIS Administrator.

Once Agency HMIS Administrators have completed required training they will be responsible for creating usernames and passwords, and monitoring HMIS access by users at their agency. With prior approval from the HMIS lead agency, this person may also be responsible for training new agency staff persons on how to use HMIS.

Client Consent Forms

In addition to posting the agency's Privacy Notice, agencies must ask clients to sign the HSN HMIS Release of Information (ROI) form. This form allows clients to authorize the electronic sharing of their personal information with other agencies that participate in HMIS when data sharing is appropriate for client service.

HMIS Software Vendor Requirements

Physical Security: Access to areas containing HMIS equipment, data and software will be secured.

Firewall Protection: The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

User Authentication: Users may only access HMIS with a valid username and password combination that is encrypted via SSL for Internet transmission to prevent theft. If a user enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security: HMIS users will be assigned a system access level that restricts their access to appropriate data.

Database Security: Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of access points; as with production servers, production databases do not share a master password database.

Technical Support: The vendor will assist HMIS Lead Agency to resolve software problems, make necessary modifications for special programming, and will explain system functionality

to HMIS Program Manager.

Technical Performance: The vendor maintains the system, including data backup, data retrieval and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

Hardware Disposal: Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures.

Confidentiality and Security

The importance of the integrity and security of HMIS cannot be overstated. Given this importance, HMIS must be administered and operated under high standards of data quality and security. HSN and HMIS Partner Agencies are jointly responsible for ensuring that HMIS data processing capabilities, including the collection, maintenance, use, disclosure, transmission and destruction of data, comply with the HMIS privacy, security and confidentiality policies and procedures. When a privacy or security standard conflicts with other Federal, state and local laws to which the partner agency must adhere, the partner agency must contact HSN to collaboratively update the applicable policies for the partner agency to accurately reflect the additional protections.

Data Assessment And Access

All HMIS data will be handled according to the following major classifications: Shared or Closed Data. HMIS staff will assess all data, and implement appropriate controls to ensure that data classified as shared or closed are handled according to the following procedures.

Shared Data

Shared data is unrestricted information that has been entered by one provider and is visible to other providers using HMIS. The HSN HMIS operates as an open system that defaults to allow shared data. Providers have the option of changing their program settings to keep client data closed.

Closed Data

Information entered by one provider that is not visible to other providers using HMIS. Programs serving particularly vulnerable populations (e.g. persons with disabilities, victims fleeing domestic violence, or individuals with HIV/AIDS), if entering client data at all, may do so

in a manner that does not share such information with other HMIS participating agencies.

Procedures For Transmission And Storage Of Data

- Open Data: This is data that does not contain personal identifying information. The data should be handled discreetly, unless it is further classified as Public Data. The data must be stored out of site, and may be transmitted via internal or first-class mail until it is considered public data.
- Confidential Data at the Agency Level: Confidential data contains personal identifying information. Each agency shall develop rules governing the access of confidential data in HMIS to ensure that those staff needing confidential data access will have access, and access is otherwise restricted. The agency rules shall also cover the destruction of paper and electronic data in a manner that will ensure that privacy is maintained and that proper controls are in place for any hard copy and electronic data that is based on HMIS data.

Whenever confidential data is accessed:

- Hard copies shall be shredded when disposal is appropriate. Hard copies shall be stored in a secure environment that is inaccessible to the general public or staff not requiring access.
- Hard copies shall not be left out in the open or unattended.
- Electronic copies shall be stored only where the employee can access the data.
- Electronic copies shall be stored where a password is required to access the data if on shared server space.

All public data must be classified as aggregated public or unpublished restricted access data.

Aggregated Public Data

Information published according to the “Reporting Parameters and Guidelines” section of these Policies and Procedures.

Unpublished Restricted Access Data

Information scheduled, but not yet approved, for publication. Examples include draft reports, fragments of data sets, and data without context or data that have not been analyzed.

Procedures for Transmission and Storage of Data

- Aggregated Public Data: Security controls are not required.
- Unpublished Restricted Access Data:
    - Draft or Fragmented Data – Accessible only to authorized HMIS staff and agency personnel. Requires auditing of access and must be stored in a secure out-of-sight location. Data can be transmitted via e-mail, internal departmental or first class mail. If mailed, data must be labeled confidential.
    - Confidential Data: Requires encryption at all times. Must be magnetically overwritten and destroyed. Hard copies of data must be stored in an out-of-sight secure location.

Data Reporting Parameters And Guidelines

All open data will be handled according to the following classifications - Public Data, Internal Data, and Restricted Data - and should be handled according to the following procedures.

Principles for Release of Data

- Only de-identified aggregated data will be released except as specified below.
- No identified client data may be released without informed consent unless otherwise specified by Florida State and Federal confidentiality laws. All requests for such information must be addressed to the owner/participating agency where the data was collected.
- Program specific information used for annual grant program reports and program specific information included in grant applications is classified as public information.
- Reports of aggregate data may be made directly available to the public.
- The parameters of the aggregated data, that is, where the data comes from and what it includes will be presented with each report.
- Data will be mined for agencies requesting reports on a case-by-case basis.
- Requests must be written with a description of specific data to be included and for what duration of time. Requests are to be submitted 30 days prior to the date the report is needed. Exceptions to the 30-day notice may be made.
- HSN reserves the right to deny any request for aggregated data.

Release Of Data For Grant Funders

Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by the HMIS Lead Agency when there is a voluntary, written agreement in place between the funding entity and the agency or program. Funding for any agency or program using HMIS cannot be contingent upon establishing a voluntary written agreement allowing the funder HMIS access.

Baseline Privacy Policy

Collection of Personal Information

Personal information will be collected for HMIS only when it is needed to provide services, when it is needed for another specific purpose of the agency where a client is receiving services, or when it is required by law. Personal information may be collected for these purposes:

- To provide or coordinate services for clients
- To find programs that may provide additional client assistance
- To comply with government and grant reporting obligations
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources

Only lawful and fair means are used to collect personal information.

Personal information is collected with the knowledge and consent of clients. It is assumed that clients consent to the collection their personal information as described in this notice when they seek assistance from an agency using HMIS and provide the agency with their personal information.

Your personal information may also be collected from:

- Additional individuals seeking services with a client
- Other private organizations that provide services and participate in HMIS

Clients must be able to access the Use and Disclosure of Personal Information policy found below.

Use and Disclosure of Personal Information

These policies explain why an agency collects personal information from clients. Personal

information may be used or disclosed for activities described in this part of the notice. Client consent to the use or disclosure of personal information for the purposes described in this notice, and for reasons that are compatible with purposes described in this notice but not listed, is assumed. Clients must give consent before their personal information is used or disclosed for any purpose not described here.

Personal information may be used or disclosed for the following purposes:

1. We collect personal information only when appropriate to provide services or for another specific purpose of our organization or when required by law. We may collect information for these purposes:
    a. to provide or coordinate services to clients
    b. to locate other programs that may be able to assist clients
    c. for functions related to payment or reimbursement from others for services that we provide
    d. to operate our organization, including administrative functions such as legal, audits, personnel, oversight, and management functions
    e. to comply with government reporting obligations
    f. when required by law
2. We only use lawful and fair means to collect personal information.
3. We regularly collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this notice.
4. We may also get information about you from:
    a. Individuals who are with you
    b. Other private organizations that provide services including, but not limited to, other agencies and programs participating in the HSN HMIS.
    c. Government agencies including, but not limited to HUD, DCF, and the Social Security Administration
    d. Telephone directories and other published sources
5. We post a sign at all client intake desks or other locations explaining the reasons we ask for personal information. The sign says: We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run

our programs, to improve services for homeless individuals, and to better understand the need of homeless individuals. We only collect information that we consider to be appropriate.

How We Use and Disclose Personal Information

1. We may or may not use or disclose personal information for activities described in this part of the notice. We assume that you consent to the use or disclosure of your personal information for the purposes described here and for other uses and disclosures that we determine to be compatible with these uses or disclosures:
    a. to provide or coordinate services to individuals. We share client records with other homeless service organizations that may have separate privacy policies and that may allow different uses and disclosures of the information. These organizations include, but are not limited to, other agencies and programs participating in the HSN HMIS.
    b. for functions related to payment or reimbursement for services
    c. to carry out administrative functions such as legal, audits, personnel, oversight, and management functions
    d. to create anonymous information that can be used for research and statistical purposes without identifying clients
    e. when required by law to the extent that use or disclosure complies with and is limited to the requirements of the law
    f. to avert a serious threat to health or safety if
        i. we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
        ii. the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat
    g. to report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence
        i. under any of these circumstances:
            1. where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law

2. if the individual agrees to the disclosure, or
3. to the extent that the disclosure is expressly authorized by statute or regulation, and
    a. we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, or
    b. if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the personal protected information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure

And

ii. when we make a permitted disclosure about a victim of abuse, neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:
    1. we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, or
    2. we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.

h. for academic research purposes
    i. conducted by an individual or institution that has a formal relationship with HSN if the research is conducted either:
        1. by an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a designated HSN program administrator (other than the individual conducting the research), or
        2. by an institution for use in a research project conducted under a written research agreement approved in writing by a designated HSN

program administrator.

And

ii. any written research agreement:
    1. must establish rules and limitations for the processing and security of PPI in the course of the research
    2. must provide for the return or proper disposal of all PPI at the conclusion of the research
    3. must restrict additional use or disclosure of PPI, except where required by law
    4. must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, and
    5. is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

i. to a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
    i. in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena
    ii. if the law enforcement official makes a written request for PPI that:
        1. is signed by a supervisory official of the law enforcement agency seeking the PPI
        2. states that the information is relevant and material to a legitimate law enforcement investigation
        3. identifies the PPI sought
        4. is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and
        5. states that de-identified information could not be used to accomplish the purpose of the disclosure.
    iii. if we believe in good faith that the PPI constitutes evidence of criminal conduct that occurred on our premises
    iv. in response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed may or may not consist only of name, address, date of birth, place of birth,

Social Security Number, and distinguishing physical characteristics, or

v. if
    1. the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), and
    2. the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

j. to comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

2. Before we make any use or disclosure of your personal information that is not described here, we will attempt to seek your consent first.
3. You have a right to an accounting of disclosures of your personal protected information. To obtain an accounting of how your PPI may have been disclosed, contact Homeless Services Network as outlined in the section regarding Privacy Grievances.

Inspection and Correction of Personal Information

1. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand. You have the right to receive these confidential communications from us as well as the right to receive them through alternative means.
2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. To inspect, get a copy of, or ask for correction of your information, you must submit your request in writing.
4. We may deny your request for inspection or copying of personal information if:
    a. the information was compiled in reasonable anticipation of litigation or comparable proceedings

b. the information is about another individual (other than a health care provider or homeless provider)
c. the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, or
d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial
6. We may reject repeated or harassing requests for access or correction.

Data Quality

1. We collect only personal information that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.
2. We are developing and implementing a plan to dispose of personal information not in current use seven years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the information.
3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

Complaints and Accountability

1. We accept and consider questions or complaints about our privacy and security policies and practices. If you think we may have violated your privacy rights or you disagree with a decision we made about access to your "Personal Protected Information" you may complete a Privacy Grievance Form, available from any Homeless Services Network staff member.
    a. It is against the law for any agency to take retaliatory action against you if you file this grievance. You can expect a written response within 30 days.
    b. Grievances must be submitted in writing and mailed to or hand delivered to: Homeless Services Network of Central Florida, 4065 LB McLeod Road Suite D Orlando, FL 32811
2. All members of our staff (including employees, volunteers, affiliates, contractors and

associates) are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.

Use Of A Comparable Database By Victim Service Providers and Youth

Victim service providers, private nonprofit agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, must not directly enter or provide data into HMIS if they are legally prohibited from participating in HMIS. Victim service providers that are recipients of funds requiring participation in HMIS, but are prohibited from entering data in HMIS, must use a comparable database to enter client information. A comparable database is a database that can be used to collect client-level data over time and generate unduplicated aggregated reports based on the client information entered into the database. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by HMIS.

Security Procedure Training For Users

All users must receive security training prior to being given access to HMIS. Security training will be covered during the new user training for all new users. All users must receive on-going annual training on security procedures from HSN.

Violation Of Security Procedures

All potential violations of any security protocols will be investigated and any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to; a formal letter of reprimand, suspension of system privileges, revocation of system privileges and criminal prosecution.

If possible, all confirmed security violations will be communicated in writing to the affected client within 14 days, unless the client cannot be located. If the client cannot be located, a written description of the violation and efforts to locate the client will be prepared by HSN HMIS staff and placed in the client's file at the Agency that originated the client's record.

Any agency that is found to have consistently and/or flagrantly violated security procedures may have their access privileges suspended or revoked. All sanctions are imposed by the HSN HMIS staff. All sanctions may be appealed to the HSN Executive Director.

Procedure For Reporting Security Incidents

Users and HMIS Support Specialists should report all unlawful access of HMIS and unlawful attempted access of HMIS. This includes theft of usernames and passwords. Security incidents should be reported to the HMIS Program Manager. The HMIS Program Manager will use the HMIS user audit trail report to determine the extent of the breach of security.

Disaster Recovery Plan

The HSN HMIS is covered under Bowman Systems' Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability, Bowman Systems provides the following disaster recovery plan. Plan highlights include:

- Database tape backups occur nightly.
- Tape backups are stored offsite.
- Seven day backup history is stored locally on instantly accessible Raid 10 storage.
- One month backup history is stored off site.
- Access to Bowman Systems emergency line to provide assistance related to "outages" or "downtime" 24 hours a day.
- Data is backed up locally on instantly-accessible disk storage every 24 hours.
- The application server is backed up offsite, out-of-state, on a different internet provider and on a separate electrical grid via secured Virtual Private Network (VPN) connection.
- Backups of the application site are near-instantaneous (no files older than 5 minutes).
- The database is replicated nightly at an offsite location in case of a primary data center failure.
- Priority level response (ensures downtime will not exceed 4 hours).

Standard Data Recovery

The HSN HMIS database is stored online, and is readily accessible for approximately 24 hours a day. Tape backups of the database are kept for approximately one month. Upon recognition of a system failure, HMIS can be copied to a standby server. The database can be restored, and the site recreated within three to four hours if online backups are accessible. As a rule, a tape

restoration can be made within six to eight hours. On-site backups are made once daily. A restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.

All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies, and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that are connected in turn to electrical circuits, which are connected to a building generator.

All client data is backed-up online and stored on a central file server repository for 24 hours. Each night a tape backup is made of the client database and secured in a bank vault.

Historical data can be restored from tape as long as the data requested is newer than 30 days old. As a rule, the data can be restored to a standby server within four hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.

For power outage, HMIS is backed up via battery back-up units, which are connected via generator-backed up electrical circuits. For a system crash, a system restore will take four hours. There is potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a tape restore is necessary. If the failure is not hard drive related, the data restore time will possibly be shorter as the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of executive management. Bowman Systems support staff helps manage communication or messaging to the HMIS Program Manager as progress is made to address the service outage.

Data Requirements

Data Collection Protocol

Partner Agencies are responsible for asking all clients a minimum set of questions for use in aggregate analysis. These questions are included in custom assessments that are created by HMIS System Administrators. The required data elements depend on the program. The mandatory data elements in each assessment are indicated in specific text indicating that the field is required.

Programs that do not adhere to the minimum data entry standards will be notified of their deficiencies and given appropriate training on how to correctly enter data. Programs that do not meet minimum data entry standards may have HMIS access suspended until such time that HMIS staff believes the program could begin to correctly enter information. After the two initial warnings from HMIS staff, a program still not adhering to the minimum data entry requirements will be made permanently inactive, and licenses will be revoked until the agency can demonstrate to HMIS staff that it is capable of maintaining minimum data requirements.

HMIS staff will submit a report to the CoC simi-annually that identifies the degree to which each all agencies within the CoC are meeting the minimum data entry standards.

The HMIS Program Manager must identify the assessments and requirements for each program, and properly set up each program in the HMIS software.

While HMIS databases are required to have the capacity to accept XML imports, HSN reserves the right to not allow XML imports into the HSN HMIS. Allowing XML imports may adversely impact data integrity and may also increase the likelihood of duplication of client files in the system.

Data Integrity And Reliability

Guidelines clearly articulating the minimum expectations for data entry for all programs entering data in HMIS will be defined in Partner Agency Agreements. HMIS Support Specialists must ensure that the minimum data elements are fulfilled for every program.

Partner agencies are responsible for the overall quality, accuracy and completeness of data entered by their staff for their clients. HMIS staff will monitor data collection for random variables and hold participating agencies accountable for not entering required data.