TENNESSEE VALLEY
COALITION for the HOMELESS

Homeless Management Information System (HMIS)

Policies and Procedures - APPENDIX

October 1, 2014

HMIS Administered by:

TENNESSEE VALLEY COALITION for the HOMELESS

business contact | 877.488.8234 **homeless assistance hotline |** 888.556.0791 **fax |** 866.876.0527
office | 4313 Ball Camp Pike, Knoxville, TN 37921 **mailing |** PO Box 1015, Jacksboro, TN 37757 **TVCHomeless.org**

Homeless Management System (HMIS) Data Quality Plan

Data Quality

Assessing the effectiveness of the current homeless service system is critical to finding successful solutions to assist and reduce homelessness. For that reason, information at project exit, such as destination and income, are important to learn if and how the system has helped to resolve clients' housing crisis and to improve their overall stability. HUD's "Housing First" model states that "Housing creates stability." Data on returning clients also contribute to this goal. Comparing project entry data with project exit data at the aggregate level will also provide a picture of homeless project impacts on the clients they serve.

The Homeless Management Information System (HMIS) staff will evaluate the quality of all HMIS member agency data on the quality (the degree to which data correctly reflects the client situation or episode as self-reported by the client) of the data entered monthly.

- All client data entered into HMIS should reflect information reported by the client, or an accurate assessment of known information by a case manager, as indicated by the 2015 HMIS Data Standards found here: **https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf**
- All client data entered into HMIS should be congruent with program details. While HUD has defined HMIS as the 'record of record', if agencies use paper-based files, they must match information entered into HMIS.

The Homeless Management Information System staff will evaluate the quality of all HMIS member agency data on the completeness of the data entered using detailed Data Quality Reports (DQRs), agency reports, and other tools utilized by local HMIS Administrators.

Data Quality Benchmarks

As stated in the 2015 HMIS Data Quality Standards issued by HUD, all contributory Homeless Assistance projects are required to follow HUD determined data quality benchmarks. These benchmarks are determined by HUD and are required. The goal of the benchmarks is to attain consistent data. The benchmarks in the following areas have been determined:

- **Timeliness**
- **Completeness**
- **Data Accuracy**
- **Program Descriptor Elements** (found in the 2015 HUD Standards Manual)
- **Annual Performance Report – Program Specific Data Elements**
- **HMIS Data Quality**

Timeliness of Data

To be most useful for reporting, the HMIS database should include the most current information on the clients served by participating homeless projects. To ensure the most up to date data, information should be entered as soon as it is collected. Timely data entry ensures that the data is accessible when it is needed, either proactively (e.g. monitoring purposes, increasing awareness, meeting funded requirements), or reactively (e.g. responding to requests for information, responding to inaccurate information). All client data must be entered within 5 business days of entry into a project.

Timeliness Requirements

a. Client information is entered within 5 business days of entry/intake into a project
b. Client information is updated regularly as information changes and at exit or annual assessment – per requirements relative to each universal and project specific data elements.
c. Clients must sign a Release of Information (must renew with the Lead Agency (TVCH) annually)

Training

Standardized training is provided by the Lead Agency HMIS Department and is vital to attaining quality data entry. Software training is performed using a standardized curriculum, presented in a consistent manner by the HMIS Department team.

a. User training will cover how to collect data, how to pass data from front-line staff to data entry staff, how to log questions about the data and how to resolve those questions, how to give feedback, and expectations for participating in user meetings. Some of these issues may be project specific, so they may need to be addressed by custom or specialized training rather than as part of the system-wide software training.
b. All users must attend a minimum of one training session annually.
    - Anyone who does not attend a required training **will be locked out of HMIS and must make arrangements with the Lead Agency HMIS Department to attend the next available training.**
    - Anyone who does not attend one training session annually **will be locked out of HMIS and must make arrangements with the Lead Agency HMIS Department to attend the next available training.**
c. New User and Refresher trainings will be conducted by the Lead Agency HMIS Department bi-monthly throughout the year.
d. Security, Privacy, Data Quality and Disaster Recovery policies will be presented annually at the first training of the calendar year.

Data Accuracy

Information entered into the HMIS database must be valid and must accurately represent the information of the individuals that enter any of the projects, therefore contributing data to the HMIS database. Inaccurate data may be intentional or unintentional. In general, false or inaccurate information is worse that incomplete information, as incomplete information can be attributed to some reasons. It is better to enter “data not collected” or “client doesn’t know” than to enter inaccurate data.

Monthly monitoring

To ensure the most up-to-date and complete data, data errors will be collected monthly, by the lead agency HMIS department and sent to each agency individually with a deadline for corrections to be finalized. The lead agency HMIS department will assist with data cleanup technical assistance when needed. Data errors will be monitored for a second time each month to assure that data errors have been corrected.

Failure to clean up data errors

Non compliance with data error correction will result in incorrect data reporting for Program Specific Reports, HMIS Annual Performance Reporting, and other Homeless Assessment Reporting required by HUD and other grant providers.

For all clients served and entered into HMIS:

A HMIS Member Agency must maintain HUD mandated data quality standards. The HUD Definitions and HMIS Policies & Procedures can be downloaded from the HMIS section of our website: **https://tvchomeless.org/hmis/hmisdownloads.**

- HMIS Member Agencies are expected to maintain no more than 5% missing data for each HUD Universal Data Element, and Program Specific Data Elements (PSDE) if applicable.
- The HMIS monthly Data Quality Reports, agency reports, and other tools utilized by local HMIS Administrators will be used to address data quality issues with the HMIS member agencies.
- HMIS staff will work collaboratively with member agencies to address and improve overall data quality.

For all clients served and entered into HMIS by a HMIS member agency:

- No more than 5% of all client level data should be “blank/not reported/null”. While these options may accurately reflect what the client has self-reported, they are considered of a low quality value.
- If an agency shows more than 5% “missing/not reported/null” then the agency must acquire this data and enter it into HMIS within the requested time period that the Lead Agency has assigned.
- Missing data will affect reports such as AHAR (Annual Housing Assessment Report) that is sent to Congress for reporting our community. An individual missing data will not be utilized in this report, and can therefore affect any funding or resources that could be awarded to our community.

- For all clients served and entered into HMIS by a HMIS member agency, all system data quality fields must be completed.

Range of missing (null) and unknown (don't know/refused) responses must be at 0%:

Data Element	Transitional Housing, Permanent Supportive Housing, Rapid Re-Housing		Emergency Shelter		Outreach Projects	
	MISSING	Don't Know/Refused	MISSING	Don't Know/Refused	MISSING	Don't Know/Refused
First & Last Name	0%	0%	0%	0%	0%	0%
SSN	0%	0%	0%	0%	0%	0%
Date of Birth	0%	0%	0%	0%	0%	0%
Race	0%	0%	0%	0%	0%	0%
Ethnicity	0%	0%	0%	0%	0%	0%
Gender	0%	0%	0%	0%	0%	0%
Veteran Status (Adults)	5%	5%	5%	5%	5%	5%
Disabling Condition (Adults)	5%	5%	5%	5%	5%	5%
Residence Prior to Entry	5%	5%	5%	5%	N/A	N/A
Zip of Last Perm. Address	5%	5%	5%	5%	5%	5%
Housing Status (Entry)	5%	5%	5%	5%	N/A	N/A
Housing Status (Exit)	5%	5%	5%	5%	N/A	N/A
Income & Benefits (Entry)	5%	5%	N/A	N/A	N/A	N/A
Income & Benefits (Exit)	5%	5%	N/A	N/A	N/A	N/A
Add' l PDEs (Adults; Entry)	5%	5%	N/A	N/A	N/A	N/A
Reason for Leaving	5%	5%	5%	5%	N/A	N/A
Destination (Exit)	5%	5%	5%	5%	N/A	N/A

The Homeless Management Information System staff will evaluate the quality of all HMIS Member Agency data on the consistency of the data entered.

- All HMIS Member Agency client data must work consistently to reduce duplication in HMIS by following workflow practices outlined in HMIS Orientation and HMIS Refresher training.

- All HMIS Member Agency client data must adhere to HMIS capitalization guidelines, so that data can be accurately understood and analyzed.
  Incorrect Capitalization:
  - ALL CAPS
  - all lower case
  - Mix OF loWEr and UPPER cAse lEtters
  - Enter nicknames in the name space (please use the Alias box).

Monitoring and Reporting Procedure

All HMIS Member Agency client data will be monitored and reported according to the dates specified on the Monitoring & Reporting Deadlines document. HMIS will provide the monitoring and reporting based on the HUD requirements, and will provide those reports to HUD and the HMIS member agency. This document can be found at: **https://tvchomeless.org/hmis/hmisdownloads**

Timeliness Measurement

The Homeless Management Information System staff will evaluate the quality of all HMIS member agency data on the timeliness of the data entered.

- All HMIS member agency client data should be entered in real-time or no later than 3 business days for CoC Funded Grants, and 24 hours for SSVF after intake, assessment, or program or service entry or exit.
- All HMIS member agency providers should back date any client data not entered in real-time to ensure that the data entered reflects client service provision dates.
- All HMIS staff, HMIS Member Agency providers, and data partners will work together to ensure the highest quality of data in HMIS.
- All agency administrators should respond to HMIS staff inquiries with in 24 business hours (1 business day).
- All HMIS member agency providers should correct client data in HMIS within 5 business days of receipt of notification of data errors.
- All HMIS staff, HMIS member agency providers, and data partners will work together to ensure accuracy of reporting and annual reporting.

Performance Measurement

- HMIS staff will measure the performance of HMIS Member Agency providers as it relates to the quality of the data entered into the system. Additionally, performance on a system-level will be measured to show the progress towards our Continuum of Care in reducing homelessness.

- HMIS staff will measure the timeliness and completeness of data entered by each HMIS Member Agency.

- HMIS staff will measure the bed utilization rates of homeless housing providers.

Data Quality Reporting and Outcomes

The HMIS Staff will send data quality monitoring reports to the Executive Director, Project Manager, and the contact person at the agency responsible for HMIS data entry. Reports will include any findings and recommended corrective actions. If the agency fails to make corrections, or if there are repeated or egregious data quality errors, the data may be thrown out in the AHAR (Annual Housing Assessment Report) sent to Congress, and therefore can affect funding and resources for our community.

HMIS data quality certification is part of several funding applications, including CoC funded projects and ESG programs. Low HMIS data quality scores may result in denial of HUD funding applications and other funding sources that required HMIS data.

Other Reporting

The HMIS staff may provide requested specialty reports to HMIS member agency providers for a fee.

Homeless Management System (HMIS) Privacy Plan

PURPOSE

This document describes the privacy plan of the Tennessee Valley Continuum of Care Homeless Management Information System (HMIS) and agencies contributing data (HMIS Partnering Agencies) to the HMIS. This document covers the processing of protected personal information for clients of HMIS Partnering Agencies.

Protected Personal Information (PPI) is any information that is maintained about a client that:

a. Allows identification of a client/consumer directly or indirectly
b. Can be manipulated by a reasonably foreseeable method to identify a specific client/consumer, **OR**
c. Can be linked with other available information to identify a specific client/consumer.

The provisions of this plan shall go into effect immediately.

DATA COLLECTION NOTICE

HMIS Partnering Agencies must let clients know that personal identifying information is being collected, and the reasons for collecting this information. To meet this requirement, HMIS Partnering agencies must post the following language in places where intake takes place:

Agency Name and its partner provider agencies collect personal information directly from you for reasons that are discussed in our NOTICE OF PRIVACY PRACTICES. Agency Name and its partner provider agencies may be required to collect some personal information by law or by organizations that provide funds to operate this project. Other personal information that is collected is important to run our projects, to improve services, and to better understand the needs of individuals being housed/sheltered/served. Agency Name and its partner provider agencies only collect information that is considered to be appropriate.

1. While the posted notice is the minimum requirement, agencies may choose to take additional steps to obtain consent from clients, including obtaining written consent. Agencies without a contractual relationship with Agency Name may use an Agency-specific alternative that complies with HUD's baseline privacy standards.

2. Each Agency should adopt and comply with the attached Notice of Privacy Practices for Use with the HMIS ("HMIS Privacy Notice"). Agencies without a contractual relationship with Agency Name may use an Agency-specific alternative that complies with HUD's baseline privacy standards.

3. Each Agency must provide a copy of the *HMIS Privacy Notice* upon client request. Clients must acknowledge receipt by signing an *HMIS Client Consent Form*. Agencies without a contractual relationship with Agency Name may use an Agency-specific alternative. The Agency must keep signed copies of the *HMIS Client Consent Form.*

4. Each Agency shall provide reasonable accommodations to persons with disabilities and to persons with limited English proficiency to ensure their understanding of the HMIS Privacy Notice and/or Acknowledgement Form.

ACCOUNTABILITY

Each agency must uphold relevant federal and state confidentiality regulations and laws that protect client records, including but not limited to the privacy and security standards found in HUD's Data and Technical Standards. If the Agency is a HIPAA-covered entity, the Agency is required to operate in accordance with HIPAA regulations and is exempt from the privacy and security standards found in HUD's Data and Technical Standards.

ACCESS AND CORRECTION

1. Each agency must allow individuals to inspect and have a copy of their personal information that is maintained in HMIS.

2. Each agency must offer to explain any information that is not understood.

3. Individuals must submit a request to inspect their HMIS data in writing to their social worker/case manager. Each agency must consider a written request for correction of inaccurate or incomplete personal information. If the agency agrees that the information is inaccurate or incomplete, the agency may delete it or may choose to mark it as inaccurate or incomplete and to supplement it with additional information.

4. Each agency may deny the individual's request for inspection or copying of personal information if:

    a. Information was compiled in reasonable anticipation of litigation or comparable proceedings
    b. Information is about another client/consumer
    c. Information was obtained under a promise of confidentiality and 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 the agency denies a request for access or correction, it must explain the reason for the denial and include documentation of the request and the reason for the denial.

6. Each agency may reject repeated or harassing requests for access or correction.

PURPOSE AND USE LIMITATIONS

Each agency will use or disclose personal information for activities described in this part of the notice. The agency assumes that clients consent to the use or disclosure of personal information for the purposes described here and for other uses and disclosures that are determined to be compatible with these uses or disclosures:

1. To provide or coordinate services to individuals (shelter, housing, case management, etc.)
2. For functions related to payment or reimbursement for services
3. To carry out administrative functions such as personnel oversight, management functions, and auditing purposes.
4. To create de-identified (anonymous) information that can be used for research and statistical purposes
5. When required by law
6. To avert a serious threat to health or safety if:
    a. the agency believes 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
    b. the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat
7. To report victims of abuse when authorized by law.
8. For research purposes unless restricted by other federal and state laws.
9. To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct).
10. For judicial and administrative proceedings in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena.
11. To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

Before any use or disclosure of personal information that is not described here, the agency must seek the clients consent first.

CONFIDENTIALITY

a. Each agency must maintain any/all personal information as required by federal, state, or local laws.

b. Each agency shall only solicit or input into HMIS client information that is essential to providing services to the client.

c. Each agency shall not knowingly enter false or misleading data under any circumstance, nor use HMIS with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.

d. Each agency shall ensure that all staff, volunteers and other persons who use HMIS are issued an individual User ID and password.

e. Each agency shall ensure that all staff, volunteers and other persons issued a User ID and password for HMIS receive confidentiality training, HMIS training, and comply with the attached *HMIS User Agreement* and the *HMIS Participation Agreement*.

PROTECTIONS FOR VICTIMS OF DOMESTIC VIOLENCE, DATING VIOLENCE, SEXUAL ASSAULTS AND STALKING

Victim service providers are prohibited from entering data into HMIS. Other agencies must be particularly aware of the need for confidentiality regarding information about persons who are victims of domestic violence, dating violence, sexual assault, and stalking. Additional protections for these clients includes explicit training for staff handling personal identifying information of the potentially dangerous circumstances that may be created by improper release of this information.

Homeless Management System (HMIS) Security Plan

1. Administrative Safeguards

A. **Security officer.** The HMIS Lead Agency (TVCH) and each Covered Homeless Organizations (CHO) must designate an HMIS security officer to be responsible for ensuring compliance with applicable security standards. The HMIS Lead must designate one staff member as the HMIS security officer. The CHO must designate the Lead Security officer of their agency.

Both Lead and CHO security officers are responsible for ensuring compliance with applicable security standards.

i. The Lead Security Officer:

1. Will provide annual training and guidance to Contributing HMIS Organization (CHO) security officers.
2. Will provide software upgrade training to all users during each software upgrade that warrants training.
3. At least twice a year will offer a security specific training for users to attend who need to renew certification of annual security training.
4. Work with Data Management Committee and CoC to develop and implement the Security Plan and review/update the plan annually.
5. Keep a current list of names and contact information for each CHO security officer.
6. Be the primary contact for the CHO security officer and work with them to resolve security issues.
7. Perform background checks on all CHO security officers and other HMIS users.

ii. The (CHO) Security Officer:

1. Will provide the CHO security officer's and each HMIS user's name and contact information to the HMIS lead security officer.
2. Ensure that all other employees in the CHO are current in their security training.
3. **Will provide new user training to current employees in the CHO.** The CHO will train new users on entry enrollment data entry, maintaining data quality, interim and updated data entry, and exit enrollments. The CHO will contact the Lead Agency HMIS department for and data quality or data cleanup assistance.
4. At least once a year the security officer will conduct a review of organization practices, policies and procedures to ensure that they are in compliance with the security plan.
5. Keep list of active users and notify Lead Agency HMIS when within 24 hours to deactivate access for employee/volunteers that no longer need access.
6. **Have an approved background check for the current calendar year.**
7. Sign and date for the current calendar year:
    a. Memorandum of Agreement
    b. User Agreement **(for themselves and for each user at the agency)**
    c. HMIS Policies & Procedures: Data Quality Plan, Privacy Plan, Security Plan & Checklist, Data Recovery Plan

iii. Both the Lead and CHO Security Officers are responsible for ensuring compliance with applicable security standards.

B. **Workforce security.** The HMIS Lead must ensure that each CHO conduct criminal background checks on the HMIS security officer and on all administrative users. Unless otherwise required by HUD, background checks may be conducted only once for administrative users.

C. **Security awareness training and follow-up.** The HMIS Lead must ensure that all users receive security training prior to being given access to the HMIS, and that the training curriculum reflects the policies of the

Continuum of Care and the requirements of this part. HMIS security training is required at least annually.

i. **Prior to being given access to HMIS, all users must:**
   1. **Participate in annual HMIS Security Training.**
      - The training will cover privacy of information, data security, data quality expectations, disaster recovery and the basics of the HMIS software. This training will be a group training webinar offered one time annually.
        i. The training will be provided by a HMIS Lead Agency Staff person for the Lead Security Officers of each CHO, current active users, and new users.
        ii. If a new user is unable to attend the annual HMIS Security Training, or is hired after the training has already occurred that year, the Lead Security Officer of the CHO will cover the required security document training listed above, and/or have the new user review the webinar video from the HMIS Security Training session for that calendar year.

   2. Visit our website for important HMIS documents and downloads. **https://tvchomeless.org/hmis/hmisdownloads.** Complete and return a copy of:
      - HMIS User Agreement
      - HMIS Memorandum of Agreement
      - Privacy Plan
      - DQ Plan
      - Security Policy & Checklist
      - Disaster Recovery Plan
   3. Complete some basic tasks in the HMIS training environment.

ii. **The HMIS lead agency will offer HMIS orientation training and HMIS refresher training on a regular basis and will make efforts to offer it more often if it is needed.**

iii. **All users of HMIS will need to participate in training that covers privacy information, data security, and data quality at least annually. The HMIS lead agency will offer this Privacy Plan, Security Policy & Checklist, Data Quality Plan, and Disaster Recovery Plan at least once a year during new user training and user refresher training.**

D. **Reporting security incidents.** Security incidents should first be reported to the CHO security officer within 2 business days of the incident. If needed the CHO security officer should then contact the HMIS lead security officer. If needed the HMIS lead security officer will bring the issue to the HMIS Data Management Committee and they in turn can bring the issue before the CoC.

E. **Disaster Recovery Plan.** In conjunction with our HMIS software Case Worthy (aka ECM), the HMIS lead agency has created a Disaster Recovery Plan found: **https://tvchomeless.org/hmis/hmisdownloads.**

F. **Annual Security Review.**
   i. **At least once a year the HMIS lead security officer and the CHO security officer will conduct an annual security review.**
   ii. **The CHO security officer security review responsibilities:**
      1. Review and complete the HMIS security check list every July
      2. Send the complete HMIS security checklist to the HMIS lead security officer.
      3. Make a plan to improve/fix all issues that were found during the completion of the HMIS security checklist.
   iii. **HMIS lead security officer security review responsibilities:**
      1. Review and complete the HMIS security check list every January.
      2. Review the completed and submitted HMIS security check lists from the CHO's.
      3. Make a plan to improve/fix all issues that were found during the completion of the HMIS security checklist.

G. **Contracts and Other Arrangements.** The HMIS lead must retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or required to comply with the requirements of this part.

2. Physical Safeguards

A. The HMIS lead agency and CHO's will take all reasonable, foreseeable and protective actions to physically secure the protected personal information of clients. Some of these actions are listed below but this list does not represent an exhaustive list of physical safeguards.

1. **To protect protected personal information, all users when transmitting written communication about clients will use the ClientID to refer to the client.**
2. **Hard copies of client information or reports with protected personal information will be kept in a locked cabinet or storage area when unattended.**
3. **Loose papers or notes with client information that are not to be stored in the client file will be securely disposed of.**
4. **The lead HMIS agency and CHO's will minimize computer/table/phone screens used to access HMIS to unauthorized individuals.**
5. **The lead HMIS agency and CHO's will turn the monitor and/or hide the screens from view during case interviews where their screens could be accidentally viewed.**
6. **Documents that contain passwords will be kept physically secure.**
7. **The servers that house HMIS information will be kept in a secured and monitored facility.**

3. Technical Safeguards

A. The HMIS lead agency and CHO's will take all reasonable, foreseeable and protective actions to technically secure the protected personal information of clients. Some of these actions are listed below but this list does not represent an exhaustive list of physical safeguards.

1. **Users will change their passwords at least once annually.**
2. **Terminals used to access HMIS will have locking screen savers and will be password protected**
3. **Browsers used to access HMIS will not use the auto fill password setting. Passwords must be manually entered each time of accessing the HMIS.**
4. **Users will not leave HMIS open and running when terminal is unattended.**
5. **Users will be automatically logged off after 30 minutes of inactivity.**
6. **Electronic Documents stored outside of a private protected local network that contain protected personal information must be password protected.**

Homeless Management System (HMIS) Security Checklist

WORKSTATION REQUIREMENTS			
REQUIREMENT	**YES**	**DOES NOT**	**FOLLOW UP ACTION**
Written Communication uses HMIS ClientID (not name)			
Hard copies of client information kept in locked cabinet (or in locked room with staff members responsible to monitor these files)			
Loose papers with client information (outside of client file) disposed of			
Monitor is turned away from a door or window, and away from client seats or outside viewing			
Documents containing passwords are physically locked or secure			
Servers housing HMIS information kept at a secured and monitored facility			

AGENCY REQUIREMENTS			
REQUIREMENT	**YES**	**DOES NOT**	**FOLLOW UP ACTION**
Notify TVCH within 24 hours of a user deactivation for user no longer employed/needing access			
Display HMIS Consent Poster near where Intake is performed			
All current users have taken HMIS Orientation Training			
Agency reports security incidents within 2 business days of occurrence			

TECHNICAL SAFEGUARDS REQUIREMENTS			
REQUIREMENT	**YES**	**DOES NOT**	**FOLLOW UP ACTION**
Terminal uses lock screen and password			
Browser accessing HMIS does not save or auto fill password			
User closes HMIS when terminal is unattended			
Electronic documents with user information uses password protection			

COMPUTER REQUIREMENTS			
REQUIREMENT	**YES**	**DOES NOT**	**FOLLOW UP ACTION**
Browser: Chrome or IE7/IE8 **			
Virus Protection			

**** Firefox is not recommended by CaseWorthy, but still works for the time being.**

- Chrome for MAC/PC can be downloaded here: https://www.google.com/chrome/browser/desktop/.
- Internet Explorer for PC here: http://www.microsoft.com/en-us/download/internet-explorer.aspx

HMIS Department Signature **Date**

PLEASE HAVE FOLLOW UP ACTIONS COMPLETED BY: **Date**

Homeless Management System (HMIS) Disaster Recovery Plan

The Tennessee Valley Continuum of Care Homeless Management Information System (TN 512-HMIS) is a critically important tool used to gather and maintain information about the homeless population in the state. This document describes the responsibilities of key personnel and three scenarios where HMIS recovery may be required:

A. On-site power outage at the Lead Agency in Knoxville
B. Local disaster in Tennessee
C. Outage or disaster at CaseWorthy (formerly ECM) location

A. On-Site Power Outage or Service Interruption

If there is a power loss at the Lead Agency, users will be able to continue normal day-to-day operations. However, reporting (including custom reporting), and technical support may be temporarily unavailable.

1. The TN 512-HMIS data is backed up nightly to an off-site, secure server bank. In the event of a disaster, this data can be immediately available via Internet connection.
2. TVCH Tech support will still be available during normal business hours.

B. Local Disaster Plan

1. Local Disaster

A local disaster is considered to be a disaster that affects locations in or around Tennessee. In the event of a local disaster:

a. TN 512-HMIS, in collaboration with the local Agencies, will provide information to local responders (fire, police, etc.) as required by law and within best practice guidelines.
b. TN 512-HMIS in collaboration with the local Agencies will also provide access to organizations charged with crisis response within the privacy guidelines of the HMIS system and as allowed by law.

2. CHO or HMIS Staff Emergency Responsibilities

During a disaster, communication between the HMIS Lead Agency staff, the CoCs, the Agencies, and the software Vendor (CaseWorthy) will be a shared responsibility that is based on location and type of disaster. Appendix A- Emergency Contacts lists key contact people and their phone numbers.

In the event of an outage or system failure, staff responsibilities include:

a. The TN 512-HMIS Project Manager or designee will notify all participating CoCs and local Agency Administrators should a disaster or major outage occur at CaseWorthy or in the TN 512-HMIS Administrative Offices.
b. When possible, the TN 512-HMIS Project Manager or designee will also provide a description of the recovery plan timeline.
c. After business hours, TN 512-HMIS staff will report system failures to the software Vendor using the after regular business hours hotline.
d. TN 512-HMIS staff will send an email to local Agency Administrators and HMIS staff no later than one hour following identification of the failure.

e. TN 512-HMIS Project Manager or designated staff will notify the HMIS Vendor if additional database services are required.
f. If an outage or failure happens at CaseWorthy, the CaseWorthy support staff will manage communication to the System Administrator as progress is made to address the service outage.

In order to ensure that HMIS data can be restored in the event of a disaster, HMIS Lead Agencies are required to:

a. Back-up internal management data systems nightly.
b. Provide a solution for off-site storage for internal data systems.
c. Perform automated backups Monday through Friday to a local network access storage (NAS) device.
d. Emergency contact information, including the names and phone numbers of local responders and key internal organization staff, designated representative of the CoCs, local HMIS Lead Agency, and the TN 512-HMIS Project Manager. See Appendix A-Emergency Contacts for a list of contacts.
e. The HMIS team is responsible for notification and nature of the emergency and the timeline of TN 512-HMIS being available.

C. Outage or Disaster at CaseWorthy (formerly ECM) Locations

1. Software Recovery Services

HMIS data is entered into CaseWorthy application. In the event that there is a service outage or disaster at CaseWorthy's location, it is important that CaseWorthy and all data is backed up and recovered as soon as possible so that personnel in Tennessee can do their work.
In addition, TN 512-HMIS has a contract with CaseWorthy that covers the following recovery and preventative options:

a. Standard System Failure Recovery
The TN 512-HMIS database is stored online, and is readily accessible approximately 24x7.

b. Data Backups
All servers, network devices, and related hardware are maintained by CaseWorthy. All client data is backed up online and stored on a central file server repository for 24 hours. Each night CaseWorthy makes a backup of client data and maintains it at a secure location.

c. Data Restores
Historical data can be restored by contacting CaseWorthy and having them restore the database within a 24 hour period.

d. System Crash Restore
After a system crash, there may the loss of all unsaved data on the current record. The HMIS system Is maintained by CaseWorthy offsite and on a secure server.

2. Major Outages

All major outages are immediately brought to the attention of TVCH executive management. CaseWorthy support staff helps manage communication as progress is made to address the service outage. CaseWorthy takes major outages seriously, and understands and appreciates that HMIS is a tool used for daily activity and client service workflow, so every effort will be made to restore service quickly.

D. Appendix – Emergency Contacts

This appendix lists the names, contact information, and email addresses for key personnel in the event of an emergency or disaster.

Name	Office Phone: (877) 488-8234	Cell Phone:	Email Address
Contact			
hmis@tvchomeless.org			
Primary Contact			
Marie Basarich	**x220**	(865) 268-9054	mbasarich@tvchomeless.org
HMIS Administrator			
Backup Management Contact			
Melanie Cordell	**x230**	(423) 494-0173	mcordell@tvchomeless.org
Chief Executive Officer			

TVCoC HMIS DOCUMENTATION
SIGNATURE PAGE

As a partnering Agency/Organization/Project in the Tennessee Valley Continuum of Care Homeless Management Information System (TVCoC HMIS), you authorized and accept responsibility for reading the HMIS HUD mandated policies, plans, other instructional information provided to you, and will ensure that all personnel with access to HMIS will also accept responsibility for familiarizing his/herself with this information.

In signing this document, you're stating that you have received the following from TVCoC HMIS Manager/System Administrator II:

1. TVCoC HMIS POLICIES & PROCEDURES
2. TVCoC HMIS DATA QUALITY PLAN
3. TVCoC HMIS PRIVACY PLAN
4. TVCoC HMIS SECURITY PLAN & SECURITY CHECKLIST
5. TVCoC HMIS DISASTER RECOVERY PLAN

_____	TN Valley Coalition for the Homeless
Agency/Program	Host Program / TVCoC Lead Agency
_____	_____
Executive Director	HMIS Administrator
_____	_____
Date Signed:	Date Signed:

---------- This copy is for the Lead Agency (Tennessee Valley Coalition for the Homeless) ----------