Standard Operating Procedures
HMIS and DV
ClientTrack

HMIS Standard Operating Procedures

Standard Operating Procedures
HMIS and DV ClientTrack

Table of Contents

1.) Overview 3

2.) Purpose of HMIS and DV ClientTrack Standard Operating Procedures 4

3.) Definitions for HMIS and DV ClientTrack Standard Operating Procedures 4

4.) Onboarding New Agencies for HMIS and/or DV ClientTrack: 7

A. Agency Partner Agreement: 8

B. Enforcement of Proper Use of the HMIS: 8

C. User Access Privileges to HMIS 9

D. Implementation Assessments: 10

E. Passwords: 10

5.) Security 11

6.) User Security 12

7.) Security Violations: 15

8.) Non HUD Funded Agencies: 16

9.) Desk and/or Onsite Monitoring: 16

10.) Agency Implementation Assessments and Denial of User or Participating Agency Access: 17

11.) HMIS Training 18

12.) HMIS User License Billing: 19

13.) HMIS Technology Requests: 20

14.) Performance and Outcomes Committee: 21

15.) Data Use and Disclosure: 22

16.) Data Access: 25

16.) IHCDA Data Processing & Preparation: 26

17.) Public Data Releases: 27

Standard Operating Procedures
HMIS and DV ClientTrack

1.) Overview

A Homeless Management Information System (HMIS) is a local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness. Each Continuum of Care (CoC) is responsible for selecting an HMIS software solution that complies with HUD's data collection, management, and reporting standards.

In 2011, IHCDA contracted with ClientTrack, Inc. (Eccovia) to provide the HMIS software. The focus of this effort was to expand participation in HMIS by homeless service providers. In 2013, IHCDA established a closed database, that is comparable to the HMIS database, to victim service providers, known as the DV ClientTrack production system. IHCDA allows agencies located in the Indiana Balance of State, and provide services to the people experiencing homelessness, to participate in the HMIS and DV production systems at no charge.

IHCDA employees at a minimum, an HMIS Manager, HMIS Trainer, and HMIS Data Analyst as staff whose primary job responsibilities are devoted to the expansion, training, and maintenance of the HMIS in the Indiana Balance of State. IHCDA HMIS staff is involved in the following activities:

- Operating the HMIS and DV ClientTrack help desk
- Creating and facilitating various types of user training
- Supporting the local Regional Council in each of the 16 regions
- Preparing and submitting the following annual reports to HUD:
    - Longitudinal Systems Analysis (formerly known as the Annual Homeless Assess Report – AHAR)
    - System Performance Measures
    - Housing Inventory Count Chart
    - Point in Time Count

The responsibility for the overall oversight of the HMIS rests with the IHCDA Board of Directors, which delegated it to the CoC Board who oversees the Performance and Outcomes Committee. The Performance and Outcomes Committee includes representatives from State agencies, academia, homeless service providers, users of the HMIS, and advocates for the homeless.

The Performance and Outcomes Committee periodically review user and executive satisfaction with the present software, discusses changes in data standards required by HUD and suggests opportunities to improve the system, especially with respect to increasing its use by non-HUD funded homeless providers.

Standard Operating Procedures
HMIS and DV ClientTrack

2.) Purpose of HMIS and DV ClientTrack Standard Operating Procedures

The purpose of these HMIS and DV ClientTrack Standard Operating Procedures is to provide guidelines, requirements, responsibilities, processes, and procedures governing the operation of the HMIS, with an emphasis on protecting the privacy of Clients and the security of Client information. These Standard Operating Procedures apply to IHCDA and HMIS Staff, Agencies, Agency Users, the HMIS Software Vendor, and any other entity involved in the administration of the Indiana BoS HMIS.

3.) Definitions for HMIS and DV ClientTrack Standard Operating Procedures

Agency: An organization working with IHCDA signing an Agency Partner Agreement thereby agreeing to follow HMIS and DV ClientTrack Standard Operating Procedures. The Agency Partner Agreement is in effect for all related programs within an Agency.

Agency Site Administrator and Deputy Site Administrator: The individuals at an Agency who are the chief liaisons between IHCDA and the Agency and whose responsibilities are more fully described in the "Agency Participation Requirements".

Agency User or User: An employee, agent, or other representative authorized by an Agency to receive an HMIS username and password.

Aggregated Data: This is data that is grouped, usually by program, but possibly across any dimension (e.g., time, region, segments of Client populations, etc.). This data type precludes exploration at a Client-identified level because all Client-level information is de-identified.

Client: A person who applies for or receives services from an Agency.

Client-level Information: A set of data records that combined represent a single Client. This type of information lends itself to more in-depth data analysis. All public Client-level Information is De-identified Information.

De-identified Information: A data set or report that removes all Protected Personal Information, (*i.e.*, information that identifies the Client by name, SSN, or other unique identifier).

Disclosure: The release, transfer, or provision of access to information outside the HMIS.

DV closed system: The closed HMIS for victim service providers where information is restricted to the assigned agency

HIPAA: The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et. seq., and its implementing regulations (all as amended).

HMIS: Homeless Management Information System — a web-based computer system managed by IHCDA staff that collects Client- identifying Confidential Information with services received and outcomes achieved by the Clients.

HMIS Contractor: Contactors involved in administering the HMIS.

HMIS Staff: IHCDA employees and/or contractors involved in administering the HMIS.

HMIS Software Vendor: ClientTrack, Inc. (Eccovia)

Minimum Necessary: The minimum amount of Protected Personal Information needed to accomplish the purpose of a request or to assess Client eligibility to provide services to the Client.

Protected Personal Information (PPI): Any information maintained by an Agency or in HMIS about a Client or homeless individual that: (i) identifies, either directly or indirectly, a specific individual; (ii) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (iii) can be linked with other available information to identify a specific individual. The term shall include Protected Health Information. This information may include demographic or financial information about a particular Client that is obtained through one or more sources. This may include information such as name, address, social security number, income, education, and housing information.

Protected Health Information: Any individually identifiable information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

Program Specific Data Elements: Additional data elements that are specific to the services provided by the Agency to each Client. Program Data are a mix of those elements required to complete the HUD APR (Annual Progress Report) and additional elements suggested by other federal agencies, HMIS practitioners and researchers.

Public Data: De-identified Information approved for release to external parties and the public. It may be either Client-level Information or Aggregated Data.

Research: An activity is defined as research when it meets the following definition: —a systematic investigation, including Research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of Research repositories and databases for Research. ‖ *(45 CFR, Part 46 — The Common Rule).* For purposes of this Policy, any use of Protected Personal Information for Research purposes must be for academic Research conducted by an individual or institution that has a formal relationship with IHCDA if the Research is conducted either: (1) by an individual employed by or affiliated with IHCDA for use in a research project conducted under a written research agreement approved in writing by the RARC; or (2) by an institution for use in a research project conducted under a written research agreement approved in writing by the RARC.

Stakeholders: IHCDA sponsors, participating agencies, programs, and people experiencing homelessness.

Universal Data Elements: Basic demographic data elements defined in the HUD Data Standards including those the Agency staff are responsible for entering into the HMIS. The 2022 HUD Data Standards are effective October 1, 2021. To review the 2022 HUD Data Standards Manual, please visit:

https://files.hudexchange.info/resources/documents/FY-2022-HMIS-Data-Standards-Manual.pdf

2022 HUD Data Standards Universal Data Elements

- Name
- Social Security Number
- Date of Birth
- Race
- Ethnicity
- Gender
- Veteran Status
- Disabling Condition
- Project Start Date
- Project Exit Date
- Destination
- Relationship to Head of Household
- Client Location
- Housing Move-In Date
- Prior Living Situation

Standard Operating Procedures
HMIS and DV ClientTrack

4.) Onboarding New Agencies for HMIS and/or DV ClientTrack:

HMIS Manager:

- Review all new agency and/or project requests submitted for HMIS and/or DV ClientTrack access to determine if the agency/project serves 100% homeless individuals and/or families
- Provides the HMIS Agency Participation Agreement for completion and signature by the agency's Executive Director
- Provides general information and the required online/on demand training links for new user access
- Assigns the new agency and/or project request to an HMIS team member
- Schedules the new agency/project onboarding meeting with the Site Administrator and Deputy Site Administrator
- Provides a comprehensive overview during the onboarding meeting to include:
    - Help Desk function
    - Indiana Balance of State HMIS and DV ClientTrack website
    - Roles/responsibilities of the Site Administrator and Deputy Site Administrator
    - HMIS Security
    - HMIS reporting
    - Data Quality
    - New User requests/forms
    - HMIS and DV ClientTrack News Page
    - Monthly live new user training opportunities

HMIS Team:

- Provides the New Project Set Up form to the agency for completion
- New Project Set Up form is reviewed for completeness
- Creates the new agency, project(s), grant(s), and services in the system.
- Set up new users in the system and provide log in credentials

Agency Site Administrator/Deputy Site Administrator:

- **Identification of Agency Site Administrator and Deputy Site Administrator:** Each Agency must identify an individual who will serve as its Site Administrator, and as needed, a Deputy Site Administrator, for setting up new user accounts and serving as a point of contact for data quality issues and corrections. Site Administrators for the HMIS play a critical role in protecting HMIS data. Time, interest, and ability are the biggest factors in determining who should be a Site Administrator for the HMIS. This title does not necessarily correspond to the

- Agency's organizational chart. The Agency User designated as the Site Administrator must also be a staff member who has an active HMIS or DV production system user account.
- The Site Administrator must attend training provided by IHCDA as needed.
- Submit the New Project Set Up request form to the help desk for new agencies and/or projects.
- Submitting new user requests to the HMIS and/or DV help desks IHCDA. This will determine appropriate access to the HMIS for each Agency User, who has been vetted by the site administrator and applicable pre-employment background checks as conducted by the Site Administrators Agency. Access to HMIS/DV ClientTrack should be based on each Agency User's job function as it will relate to the HMIS and DV production systems data entry and retrieval (*i.e.*, role-based security).
- Detecting and responding to security violations, and data quality errors of HMIS policies or Agency policies and procedures.
- In conjunction with IHCDA, decisions regarding the issuing, altering, and revoking of HMIS access privileges.
- Ensuring system auditing (within the Agency) via running the data quality report for each agency, at minimum quarterly as stated in the HMIS/DV Data Quality Plan.
- Serving as the point of contact and agency individual for working with agency end users to correct data quality errors
- Ensuring Agency-wide data quality.
- Ensuring the security of the HMIS on the Agency website.
- Notifying IHCDA staff of any security breach within twenty-four (24) hours of the breach.
- Enforcing Agency information system policies and standards.

A. Agency Partner Agreement:

The Executive Director or authorized official must sign the **HMIS or DV Participation Agreement**, which confirms the Agency's commitment to comply with the policies and procedures for using the HMIS open system or DV closed system in collaboration with IHCDA.

B. Enforcement of Proper Use of the HMIS:

All Agency Users must sign the **HMIS User Agreement/Code of Ethics for HMIS Providers or the ClientTrack User Code of Ethics for Victim Service Providers** and comply with the terms contained in the agreement whether the User is a staff member, volunteer or consultant prior to

the Agency User receiving HMIS training and a password to the HMIS. A copy of the **HMIS User Agreement/Code of Ethics for HMIS Providers or the ClientTrack User Code of Ethics for Victim Service Providers** must be sent to IHCDA and IHCDA will maintain a copy of it. Violation of this agreement may be considered a violation of the Agency User's employment with the Agency, and could result in disciplinary action, up to and including termination of the Agency User's employment or affiliation with the HMIS as well as potential personal civil and criminal legal fines and penalties. The current **HMIS User Agreement/Code of Ethics for HMIS Providers or the ClientTrack User Code of Ethics for Victim Service Providers** is posted at: https://www.in.gov/ihcda/indiana-balance-of-state-continuum-of-care/hmis-clienttrack-and-dv-clienttrack/

C. User Access Privileges to HMIS

Agency User access and access levels may be determined by the executive leadership of the Agency in consultation with the Agency Site Administrator/Deputy Site Administrator and IHCDA HMIS Manager. HMIS Staff will generate a username and password for each Agency User, who will be required to generate a unique password his or her first time accessing the HMIS. The Agency User should be the only person, who will know his or her unique password.

Agency Users:

- Read and sign the **HMIS User Agreement/Code of Ethics for HMIS Providers or the ClientTrack User Code of Ethics for Victim Service Providers** when joining an Agency and as directed by IHCDA based on policy updates.
- Agency Users are bound by the **HMIS User Agreement/Code of Ethics for HMIS Providers or the ClientTrack User Code of Ethics for Victim Service Providers** and the **HMIS Participation Agreement** and must comply with same. All Agency Users have a critical role in the effort to protect and maintain Client information contained in the HMIS.
- Agency workstations should be configured to automatically turn on a password protected screen saver when the workstation is temporarily not in use.
- Agency Users must log off the HMIS or lock their workstation when leaving their workstation and close the Internet browser to prevent someone else from viewing the last Client screen.
- Support compliance with all federal and state statutes and regulations.
- Maintain the confidentiality, privacy and security of PPI that have collected or for which Agency Users have been given access privileges
- Accept responsibility for all activities associated with the use of their Agency User accounts and related access privileges.

- Report all suspected security and/or policy violations to an appropriate authority at the Agency (e.g., manager, supervisor, system administrator or the HMIS Security Officer). Utilize the security incident report form and send in writing to the HMIS Team at IHCDA.
- Review the HMIS Notice of Privacy Practices, the HMIS Statement of Privacy Practices and the HMIS Policies and Standard Operating Procedures.
- Attend all trainings required by IHCDA HMIS policies and guidance.
- Follow all specific policies, guidelines and procedures established by the Agency with which they are associated and that have provided them access privileges.
- Persons who violate this policy may be denied access to HMIS and may be subject to other penalties and disciplinary action. The Agency should have documented procedures in place for issuing, altering, and revoking access privileges on shared systems. Any Agency User's right to access the HMIS shall be at IHCDA's sole discretion.

IHCDA User Access:

- Only IHCDA staff needing information from the HMIS for legitimate business purposes shall be given access rights. Prior to being given access rights, he or she shall be trained on HMIS privacy and security policies and sign/complete the HMIS User Agreement/Code of Ethics for HMIS Providers or the ClientTrack User Code of Ethics for Victim Service Providers **and new user training via online webinar or on demand learning management system**.

D. Implementation Assessments:

Agencies may be monitored/ audited on compliance with the procedures outlined in HUD's HMIS Data and Technical Standards and the policies and procedures contained herein.

E. Passwords:

- An Agency shall only permit access to HMIS with use of an Agency User authentication system consisting of a username and a password which the Agency User may not share with others. Temporary passwords are created when a new Agency User is created.
- The Agency User will be required to change the password the first time he or she logs into the system. Passwords are the individual's responsibility and Agency Users cannot share passwords and passwords should be stored securely and not be accessible to other persons. Passwords should never be stored or displayed in any publicly accessible location. Passwords should be designed to prevent any Agency User from being able to log onto more than one (1)

workstation at a time, and to prevent any Agency User from being able to log onto the network from more than one (1) location at a time.

- The password must be between 8 and 12 characters and contain a mix of alpha and numerical, and special characters (alphanumeric). Passwords should not use or include the User's username, the HMIS name, or the HMIS Software Vendor's Name. Passwords should not be easily guessed or consisting entirely of any common word found in any dictionary (spelled in correct or reverse order).
- Passwords should be changed periodically by each Agency User. IHCDA requires that HMIS passwords are changed at least every ninety (90) days.
- The Agency Site Administrator must immediately notify IHCDA staff of the any Agency User's termination to allow IHCDA staff to terminate the Agency User's access rights. If a staff person is planning to go on leave for a period of longer than forty-five (45) days, their password should be inactivated immediately upon the start of their leave. User accounts will automatically terminate after thirty days of inactivity.

5.) Security

- To protect the availability, security, and integrity of the HMIS, all computing systems (including, without limitation, networks, desktops, laptops, mini-computers, mainframes, and servers) accessing the HMIS or containing personal protected information shall comply with the minimum security measures and practices outlined herein.
- The procedure for client data generated from the HMIS shall be that electronic data shall be stored in a binary, not text, format. Protected Personal Information shall be stored in an encrypted format using at least a 128-bit key. Regarding raw data: Agency Users who have been granted access to the HMIS report functionality have the ability to download and save Client level data onto their local computer. Once this information has been downloaded from the HMIS in raw format to an Agency's computer, this data becomes the responsibility of the Agency. An Agency must develop a protocol regarding the handling of data downloaded from the report writer, record disclosure and storage.
- The HMIS is a secure database which allows twenty-four (24) hour access to all qualified Users. The Agency must develop and enforce policies and procedures to address the following areas of data security and integrity:
- In order to ensure that unauthorized persons cannot physically access servers, physical security measures and objectives will be implemented where applicable and appropriate to protect HMIS computing and network assets. As with logical security measures at IHCDA, physical security measures required for protecting the HMIS computing resources shall be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved. The more sensitive and critical the computing environment, the more control measures are likely to be used.

Because HMIS will be collecting and storing sensitive information, physical access control measures sufficient to prevent the HMIS from unnecessary and unauthorized access, use, misuse, vandalism, or theft must be implemented. All specific tools, systems, or procedures implemented to meet physical security requirements should be selected based on its cost-effectiveness and common sense.

- IHCDA's HMIS Software Vendor and data custodian shall provide the following security, as well as follows all other security measures set forth herein:
    - HMIS data shall be copied on a regular basis to another medium (*e.g.*, tape) and stored in a secure off-site location. Ideally, the regular copying will be via continual redundant backups.
    - Off-site storage shall include fire and water protection for the storage medium.
    - Surge suppressors shall protect physical systems for collecting and storing the HMIS data.
    - Central server, mainframe or minicomputer shall store the central hardware in a secure & locked room with an uninterrupted power supply, a raised floor, and appropriate temperature control and fire suppression systems.
    - Electronic data transmission transmitted over publicly accessible networks or phone lines shall be SSL encrypted to at least 128-bit encryption.
    - Electronic data shall be stored in a binary, not text, format. Protected Personal Information shall be stored in an encrypted format using at least a 128-bit key.
    - Access to the physical system shall be controlled.
    - Network redundancy built into central server site and/or alternate site.
    - Staff on site or on call 24 hours a day and 7 days a week.
    - Server firewall and virus protection shall be maintained and kept current.

6.) User Security

- **Agency Policies Restricting Access to Data:** Each Agency must establish internal access to data protocols. These policies must govern who has access, for what purpose, and how the information can be transmitted. Other issues that should be addressed include storage, transmission, and disposition of this information. Agencies must have written policies and procedures in place regarding the appropriate access to Client data in the HMIS and its obligations herein under the **HMIS User Agreement/Code of Ethics for HMIS Providers or the ClientTrack User Code of Ethics for Victim Service Providers**. The policies must include, without limitation, when, where and under what circumstances it is deemed appropriate for Agency staff to access HMIS data outside

the office. The policies must also indicate the consequences for an individual's failure to abide by these policies.

- Agency Users who have been granted access to the HMIS report functionality have the ability to download and save Client level data onto their local computer. Once this information has been downloaded from the HMIS in raw format to an Agency's computer, the data then become the responsibility of the Agency. An Agency must develop protocols regarding the handling of data downloaded from the report writer, and disclosure and storage of these records.
- The HMIS software will automatically log off after a pre-set interval of inactivity.
- The use of the HMIS always constitutes an express consent to the monitoring of system use and security. If such monitoring reveals possible violations of the law, pertinent information will be provided to law enforcement officials. Any persons using HMIS or information obtained from this application without proper authorization or in violation of these policies and procedures may be subject to civil and/or criminal prosecution. Any persons enabling access by an unauthorized individual may also be subject to internal disciplinary actions in addition to civil and/or criminal prosecution.
- These policies are applicable to all HMIS users (employees, contractors, and others) in all agencies, partners and funders and the computer systems, networks, and any other electronic processing or communications and related resources used in conjunction with the IHCDA HMIS system and/or data obtained through the HMIS system.
- Each person with access to confidential information must understand their personal responsibility to maintain its confidentiality. Client information must be protected so that it cannot be modified while in transit or storage. Reported data must be accurate. If an employee leaves your agency, inform IHCDA within one (1) business days that their account needs to be deactivated.
- Users may not electronically transmit unencrypted client data across a public network. Users must use the following procedures:
    - Data extracted from HMIS and stored locally will be stored in a secure location and will not be transmitted outside of the private local area network unless it is properly protected.
    - Personal identifiable client data will not be distributed through email, this includes when submitting tickets to the Help Desk.
    - User must clear browser history once he or she logs out of HMIS
    - Do not allow the browser to save password.
    - Any security questions can be addressed to the HMIS System Administrator.

Media and Hard Copy Protection: The Agency must secure any electronic media or hard copy containing identifying information that is generated either by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. Any paper or other hard copy generated by or for the HMIS that contains identifying information must always be supervised

when it is in a public area. If Agency staff is not present, the information must be secured in areas that are not publicly accessible in a secure manner (*e.g.*, locked filing cabinet or locked office). Agencies wishing to dispose of hard copies containing identifying information must do so by shredding the documents or by other equivalent means with approval by IHCDA. In addition, in order to delete data from a data storage medium, the Agency must have procedures that require the reformatting of the storage medium. The data storage medium should be reformatted more than once before reusing or disposing of the medium.

Agency User Authentication: Authorization is the provision of specific permissions or authority to have access. Access control measures required for establishing Agency Users' access to any HMIS computing resources shall be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved. All Agency Users' system access must be based on the —principle of least privilegeǁ and the —principle of separation of duties.

There will be multiple levels of access to the HMIS. The appropriate access to the HMIS is determined for each Agency User. This determination is to be based on each Agency User's job function as it will relate to the HMIS data entry and retrieval and will be officially designated by the Site Administrator.

The HMIS will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent the interception of critical or sensitive information.

Confidentiality: The HMIS preserves confidentiality by encrypting the data sent over the Internet. In addition, the Agency must make every effort through its policies and procedures to ensure that any PPI collected remains confidential, especially at the intake point.

Any staff, volunteer or other person who has been granted an Agency User ID and password and has committed a breach of security of HMIS and/or Client confidentiality may be subject to sanctions including but not limited to a warning or revocation of HMIS access rights. A revoked Agency User may be subject to discipline by the Agency pursuant to the Agency's personnel policies.

Federal, state, and local laws seek to protect the privacy of persons with physical and/or mental illness, who have been treated for alcohol and/or substance abuse, have been diagnosed with HIV/AIDS. Agencies who serve these protected classes of clients, may hide the Client's case notes, diagnoses, and treatment from other agencies using the HMIS. The Agency is encouraged to seek its own legal advice in the event of requests of this PPI by other agencies.

Integrity: Integrity provides assurance of an unaltered or unmodified state of information. All systems are required to have the capability to log basic information about an Agency User and access activity and for the possible creation of historical logs and access violation reports. The Agency Executive User should review audit reports periodically to ensure appropriate privacy

and data access policies are being followed. Deviations from policy should be reported to IHCDA within twenty-four (24) hours of discovering the inappropriate access.

Availability: Availability ensures that there is no delay or denial of authorized services or loss of data processing capabilities. This takes into account things such as virus protection, firewalls, intrusion detection, management of operating system updates, backup and recovery, and physical security to make sure that HMIS is available to be used by Agency Users.

Computer Operating System Maintenance: Agencies must have a plan to keep the computers used to access HMIS updated with the latest security and other updates recommended for the operating system. The local and server network computers must have automatic updates on every computer that accesses HMIS.

Firewalls and Virus Protection: Agencies must have firewall protection on its networks or computers providing a barrier between the organization and any systems, including the Internet and other computer networks, located outside of the organization accessing the Internet and the application. For example, a workstation that accesses the Internet directly through a modem would need a firewall; however, a workstation that accesses it through a central server would not need a firewall as long as the server has a firewall.

Virus protection must also be in place employing commercially available virus protection software that includes automated scanning of files as they are accessed by Agency Users on the system where the HMIS application is housed. Each Agency and IHCDA must also subscribe to virus software, as well as an updates subscription to maintain the virus definitions and code base.

Personnel Security Measures: Agencies must establish and maintain all necessary processes and procedures to properly and immediately close and remove all system and network privileges and resources when an employee is terminated including notifying IHCDA to disable the account within 24 hours or one (1) business day.

Disaster Protection and Recovery: The HMIS is redundantly and physically backed up by the HMIS Software Vendor in accordance with all current HUD requirements. It is recommended that larger Agencies consider their own back up of any HMIS data maintained on site. All Agencies should have a disaster plan that allows uninterrupted business access to the Internet for the purposes of the HMIS despite fire, flood, or other disaster.

7.) Security Violations:

- ***All security breaches must be reported first to the HMIS Team within 24 hours.*** As appropriate, IHCDA legal department will be made aware of the situation. The Attorney General will be notified if any social security breaches are made as required by Indiana law.

- Upon notification of a security breach, the IHCDA HMIS Team will investigate the report. IHCDA's systems analyst, currently At Work Solutions, will investigate the technical issues in collaboration with IHCDA's IT department. The system's analyst will document the situation and how the problem has been corrected. Testing will be conducted to ensure that the problem has been resolved. If the security breach involves PPI, IHCDA's legal department will be notified and will provide guidance on any specific actions that need to be taken by the Agency.
- IHCDA will report and respond to security incidents by following HUD-determined predefined threshold when reporting is mandatory, as established by HUD.
- If during the cost of auditing it is determined that an Agency has a HMIS policy or security violation, the Agency must respond to IHCDA in writing within 10 working days after being notified of the HMIS Policy Violation (breach in security) or the incident is discovered by the Agency. The Agency must inform IHCDA of how it has addressed the violation. Failure to comply with HMIS requirements may result in IHCDA withholding program payments or termination of the grant(s) until compliance is completed and documented. . In addition, failure to comply with requirements may result in an Agency being ineligible for funding or receiving a low HMIS performance score in the next grant year.

8.) Non-HUD Funded Agencies:

- Agencies that are not funded by HUD programs but utilize HMIS must comply with the same policies and procedures as Agencies that are funded by HUD. Failure to comply may result in termination of the Agency's access to HMIS.

9.) Desk and/or Onsite Monitoring:

- IHCDA staff will monitor HMIS participation through periodic and annual desk and/or onsite security reviews to ensure the implementation of the security requirements. Additionally, data in HMIS will be reviewed regularly. Data will be reviewed within the reimbursement process for HUD sponsored permanent supportive housing programs. IHCDA reserves the right to withhold payment until HMIS violations are corrected or required levels of data quality are achieved.
- IHCDA will also review data quarterly for all other BoS CoC HUD Grantees. Data quality and project performance will be reviewed by the CoC for all projects.

- IHCDA will provide a security audit checklist for the security reviews to provide Agencies with expectations for monitoring. The goal of the audits is to ensure that Agencies are complying with security requirements. IHCDA will work with agencies that receive findings to ensure they are remedied as quickly as possible for the benefit of all Agencies who utilize HMIS.
- **Consequences of Security Violations:**
    - First time offense - Findings will be assessed for the security breach. These issues must be resolved by the date specified by IHCDA. The Agency may be warned and/or additional training may be required.
    - Second time offense – The Agency's access to HMIS may be suspended, points may be taken away from current or future funding applications, or an Agency may be required to assign the right to use/ enter their Clients information to another individual or entity

10.) Agency Implementation Assessments and Denial of User or Participating Agency Access:

- Agencies are responsible for understanding and ensuring that their Agency Users abide by the following policies posted on Indiana Balance of State Continuum of Care - HMIS and DV ClientTrack
    - **HMIS Privacy Practices Notice**
    - **HMIS Statement of Privacy Practices**
    - **HMIS Standard Operating Procedures**
    - **HMIS User Agreement/Code of Ethics for HMIS Providers**
    - **DV ClientTrack User Agreement Code of Ethics for Victim Service Providers**
    - **HMIS Participation Agreement**; and
    - Any other policies or guidance issued by IHCDA.

  Agencies must pass the Security Audits performed by HMIS Staff or perform remedial actions that are required to pass the Security Audits within the time period provided requested by IHCDA.

  Agencies may self-assess by downloading the current Security Audits Checklist on Indiana Balance of State Continuum of Care - HMIS and DV ClientTrack

IHCDA HMIS Staff: IHCDA shall perform random Security Audits following the **Security Audit Checklist**. These audits may occur in conjunction with other monitoring or inspections performed by IHCDA that is not specific to the HMIS.

- IHCDA shall call the Executive Director or Site Administrator to arrange a time to meet. If the Executive Director or the Site Administrator is not available, another Agency staff member familiar with the HMIS operation should accompany IHCDA during the Implementation Assessment.
- Violations of security or privacy protocols will be investigated by the Agency and HMIS Staff.
- All confirmed violations of a breach of a Client's PPI will be communicated in writing by the Agency to the affected Client within fourteen (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 the Agency and sent to IHCDA and placed in the Client file at the Agency.
- If the Agency fails the audit and follow up work is required, the proposed next audit date will be negotiated, and the corrective actions will need to be completed prior to the next Implementation Assessment.
    - Any Agency User found to be in violation of security protocols may be sanctioned accordingly. Sanctions may include but are not limited to: submission of a plan of correction, a formal letter of reprimand, suspension of HMIS privileges, revocation of HMIS privileges, termination of the HMIS Participation Agreement, and civil or criminal prosecution.
    - All sanctions will be imposed by IHCDA.
    - All sanctions may be appealed to the Performance and Outcomes Committee to receive a non-binding advisory opinion on whether the sanction is appropriate. In all cases, IHCDA retains the final discretion and authority to impose sanctions.
    - Additional sanctions may be imposed by funders.

Notwithstanding these Implementation Assessments and other auditing performed by IHCDA and the procedures described herein, IHCDA may take action for violation of the procedures described herein even if the violation is discovered by IHCDA through other means.

11.) HMIS Training

HMIS Staff are the primary responsible party for training Agency Users. The training administered by HMIS Staff is required by all HMIS users bi-annually, as verified by registration for and attendance at a scheduled webinar training, or in person training hosted by IHCDA. Training webinars are offered on a variety of topics and to audiences that include new users and advanced users interested in executive level reports and/or preparation of required Annual

Progress reports or other reports required by HUD. HMIS trainers include IHCDA staff, representatives of Eccovia, and other contracted consultants.

New Users: Prior to issuance of a user password each new user must complete the User Agreement/Code of Ethics and return it to IHCDA, preferably via email. Upon receipt and after training, HMIS Staff will issue a username and initial password. All users are expected to be active on the HMIS and to attend training annually.

Established Users: All HMIS users are required to attend at least one (1) training session bi-annually. The training topic must include security training.

Training: Participation in training will be evidenced by the attendance reports maintained for online webinars and/or sign in sheets at live trainings. Any Agency User found to be logging in to training but not actively following the session, as evidenced by electronic monitoring of alternate key stroke activity, failure to connect and other open windows, will be required to repeat the training.

12.) HMIS User License Billing:

Agencies serving the Homeless shall have access to the IHCDA maintained HMIS free of charge. There is no requirement that an agency receive HUD or other federal or state funds to participate in the HMIS. IHCDA reserves the right to charge a reasonable fee for the use of the HMIS for other purposes. *All agencies receiving HUD funding are required to utilize the HMIS system or a comparable database which meets all of the HUD HMIS System Requirements for data and reporting.*

The U.S. Department of Housing and Urban Development (HUD) and the federal partners, along with other planners and policymakers use aggregate Homeless Management Information System (HMIS) data to better inform homeless policy and decision making at the federal, state, and local levels.

The HEARTH Act, enacted into law on May 20, 2009, requires that all communities have an HMIS with the capacity to collect unduplicated counts of individuals and families experiencing homelessness. Through their HMIS, a community should be able to collect information from projects serving homeless families and individuals to use as part of their needs analyses and to establish funding priorities. The Act also codifies into law certain data collection requirements integral to HMIS. With enactment of the HEARTH Act, HMIS participation became a statutory requirement for recipients and subrecipients of the Continuum of Care (CoC) Program and Emergency Solutions Grant (ESG) funds.

> **Billing:** Any billing of User licenses by IHCDA that occurs related to use of the HMIS will be in accordance with this section.

Terminating of User Licenses: Refunds or partial refunds will not be given to any Agency when a User license is terminated due to a violation of HMIS policies and procedures. Refunds or partial refunds will not be given to any Agency when a User license is terminated in the middle of the twelve (12)-month billing cycle for that license except at IHCDA's sole discretion and in the case of rare and extenuating circumstances.

Transferring User Licenses: Agencies may terminate one (1) User license and add another license simultaneously without disrupting the billing cycle or incurring any additional costs. For example, if an Agency User needs to take a leave of absence, another Agency User can be added during that time period.

- All licenses that are transferred must have a new username and password created.
- All Agency Users must sign the **User Agreement/Code of Ethics** and return a copy the agreement to IHCDA prior to receiving a username and password.
- All new Agency Users must attend HMIS training. Training may be provided onsite by an individual authorized by IHCDA. Agency User may also attend one of IHCDA's training sessions.

Cancellation of User License: Agencies may cancel a User license within thirty (30) days of its creation, or within thirty (30) days of receiving an invoice for a User license, at no charge.

- Agencies that cancel User licenses may be assessed fees that have been previously waived, such as training fees and setup fees.

13.) HMIS Technology Requests:

Agency must complete and submit a technology request via e-mail.

- IHCDA will review and consider the request. Technical requests not requiring additional funds will be evaluated by HMIS Staff and responded to directly. When the request involves the purchase of equipment and/or costs related to outside consultation, it will be reviewed by IHCDA on a case-by-case basis
- If the request for funding is approved, the Agency may incur the cost and/or submit documentation to IHCDA for reimbursement.
- IHCDA will review all requests and develop a timeline for approval and implementation.
- Incomplete or denied requests may be resubmitted.

14.) Performance and Outcomes Committee:

The performance and outcomes committee will review the Homeless Management Information System (HMIS) data, identify common themes, and provide support to improve data quality and system performance measures (SPM) during the competitive process. The committee will look at how HMIS is performing and if recommendations should be made to change vendors. The committee will also look how data collected can be used to improve programs and inform the public.

- **Operations:** The committee will focus on the impact of the overall system data on the Continuum of Care (CoC) including CoC projects, Emergency Shelter Grant (ESG) projects and the Point In Time (PIT) count.
- **Committee Strategic Objectives:**
    - Ensure the BoS can perform in the top 25% of NOFA
    - Reduce the Point In Time (PIT) count by 5%
    - Increase the number of youth counted in the Point In Time (PIT) count by 2 %
    - Identify agencies that need improvement and those that are high performing based upon metrics.
    - Reduce number of individuals who are homeless for the first time by 5%
    - Increase the percentage of housing project applications using the Housing First model by 5%
    - Increase the percentage of people who exit to or retain permanent housing
    - Increase number of high performing agencies by 2 %
    - Recommend new uses for data that can support the work of the agencies and inform the public about homelessness
    - Create funding opportunities for new projects by identifying those agencies that are not utilizing funding or system currently
- **Chairperson Responsibilities:** The Chair is responsible for calling, planning, and presiding over committee meetings. Currently meetings are held on the second Tuesday of every month via conference call. The chair reviews the previous board minutes, calendar of activities or reported issues needing to be addressed to create the monthly agenda. The secretary takes and maintains committee minutes. The secretary will serve for one year, nominated and voted on by committee members.
    - Supply meeting space for Performance & Outcomes committee meetings
    - IHCDA to host and arrange conference line for monthly meetings for individuals who are unable to attend in person meeting
- **IHCDA Staff Responsibilities:** IHCDA staff involved with HMIS, collaborative applicant and ESG work will notify the Chair about issues or information of importance that requires Performance & Outcomes Committee attention in a timely fashion.

15.) Data Use and Disclosure:

Each HMIS Stakeholder has certain rights and responsibilities regarding the data collected within the HMIS.

- **HMIS Sponsors:** HMIS sponsors have rights to all De-Identified Public Data produced through the HMIS. Sponsors are:
    - United States Department of Housing and Urban Development
    - Indiana Housing and Community Development Authority
- **HMIS Staff:** HMIS Staff is responsible for the proper collection and dissemination of information among the HMIS Stakeholders. The HMIS Staff is responsible for ensuring that all Client information is fully protected, and that all data use conforms to IHCDA adopted policies.
- **Agency Users:** Agency Users are also responsible for ensuring that all Client information is fully protected, and that all data use conforms to IHCDA adopted policies.
- Agencies and Programs: Agencies sign the **HMIS Participation Agreement** (posted on Indiana Balance of State Continuum of Care - HMIS and DV ClientTrack) pledging their agreement and support of all policies. Agencies also agree to post the **HMIS Statement of Privacy Practices** that defines the right of Clients.
- **ALLOWABLE USES AND DISCLOSURES OF PROTECTED PERSONAL INFORMATION ("PPI"):**
    - **Privacy Documents:** The **HMIS Notice of Privacy Practices** describes why personal information is being collected. It also refers Clients to the **HMIS Statement of Privacy Practices** for additional information regarding how their information may be used or disclosed. The **HMIS Statement of Privacy Practices** describes how information about Clients can be used and disclosed and how Clients can access their information.
    - **Routine Uses and Disclosures:** PPI in the HMIS may be used and disclosed under the following routine circumstances:
        - **Coordination of Services:** PPI may be used and disclosed to provide or coordinate services to a Client.
        - **Payment:** PPI may be used and disclosed for functions related to payment or reimbursement for services.
        - **Administrative Functions:** PPI may be used and disclosed to carry out administrative functions, including, but not limited to legal, audit, personnel, oversight, and management functions.
        - **Creating De-Identified PPI:** PPI may be used and disclosed to create De-identified Information.
        - **Other Permissive Disclosures:** The following additional uses and disclosures recognize those obligations to disclose PPI by balancing competing interests in a responsible and limited way. These additional

uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this paragraph modifies an obligation under applicable law to use or disclose PPI. The following uses and disclosures of PPI may only be made upon the approval of the Executive Director of the Agency and in consultation with IHCDA:

- **Uses and Disclosures Required by Law:** PPI may be used and disclosed when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.
- **Uses And Disclosures To Avert A Serious Threat To Health Or Safety:** PPI may be used and disclosed, consistent with applicable law and standards of ethical conduct, if: (1) IHCDA, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health and safety of an individual or the public; and (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
- **Uses And Disclosures About Victims Of Abuse, Neglect Or Domestic Violence:** PPI about an individual whom agency staff reasonably believes to be a victim of abuse, neglect or domestic violence may be disclosed to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect, or domestic violence under any of the following circumstances:
    - Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
    - If the individual agrees to the disclosure; or
    - To the extent that the disclosure is expressly authorized by statute or regulation; and the agency believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or 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 PPI 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.

If such a permitted disclosure about victims of abuse, neglect or domestic violence is made, staff must promptly inform the individual that a disclosure has been or will be made, except if: (1) the Executive Director of the Agency, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or (2) staff would be informing a personal representative (such as a family member or friend), and the Executive Director of the Agency reasonably believes 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 determined by the Executive Director of the Agency, in the exercise of professional judgment.

- **Uses and Disclosures for Academic Research Purposes:** PPI may be used and disclosed for academic research conducted by an individual or institution that has a formal relationship with IHCDA if the research is conducted either:
  - 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 the Program Director (other than the individual conducting the research); or
  - By an institution for use in a research project conducted under a written research agreement approved in writing by the Program Director.
  - All uses and disclosures for Research purposes shall comply with subsection E below ("IHCDA HMIS Research Policy"). Further, a written research agreement must: (1) establish rules and limitations for the processing and security of PPI in the course of the research; (2) provide for the return or proper disposal of all PPI at the conclusion of the research; (3) restrict additional use or disclosure of PPI, except where required by law; and (4) require that the recipient of data formally agrees to comply with all terms and conditions of the agreement. A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board, or other applicable human subject's protection institution.
- **Disclosures for Law Enforcement Purposes:** PPI may be disclosed, consistent with applicable law and standards of ethical conduct, for a law enforcement purpose to a law enforcement official under any of the following circumstances:

- In response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer, or a grand jury subpoena;
    - If the law enforcement official makes a written request for protected personal information 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.
    - If IHCDA believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of IHCDA or an HMIS Agency;
    - 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 consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or
    - 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.

16.) Data Access:

HMIS Staff may have access to all data types (including, but not limited to PPI) as necessary to perform their functions for the HMIS and consistent with the Routine Uses and Disclosures listed in "A" above. HMIS Staff must pass a background check and sign the **HMIS User Agreement/Code of Ethics for HMIS Providers and/or ClientTrack User Agreement/Code of Ethics for Victim Service Providers**.

- **HMIS Sponsors' Representatives:** HMIS sponsors' representatives may receive reports containing Public Data.
- **HMIS Subcontractors and Vendors:** HMIS subcontractors and vendors have access to all data types as necessary to perform their functions for HMIS consistent with the Routine Uses and Disclosures listed in "A" above. HMIS subcontractors and vendors must agree in writing to maintain the confidentiality of all data received from HMIS.
- **HMIS Agencies and Programs:** Agency and program staff have access to their own Agency's/program's data, as bound by these HMIS Policies and Standard Operating Procedures. Agency and program staff must sign the **HMIS User Agreement/Code of Ethics for HMIS Providers and/or ClientTrack User Agreement/Code of Ethics for Victim Service Providers** and agree to follow these Policies and Standard Operating Procedures. HMIS Agencies and programs may also have access to Public Data and PPI submitted by other Agencies for purposes of providing services to a Client (with implied Client consent), except under circumstances where federal or state law requires additional restrictions or confidentiality protections.
- **Access to Data for monitoring:** A regional CoC representative may have access to Agency data for the express purpose of monitoring and aggregate reporting purposes for regional review. A current and signed MOU must be in place for a regional CoC representative to have access to data for an Agency.
- **Researchers:** Researchers may have access to PPI and De-identified Information only in accordance with the approval procedures set forth below in "E" ("IHCDA HMIS Research Policy").
- **Other Third Parties:** Data may be disclosed to other third parties (*e.g.*, media requests) only in accordance with the approval procedures set forth below in "D" ("Public Data Releases").

16.) IHCDA Data Processing & Preparation:

IHCDA may or may not do the following:

- **Cleaning:** Data cleaning may be performed by HMIS Staff, a subcontractor, or another IHCDA vendor. During this process the data is reviewed for completeness, adherence to the data schema (data types and answer ranges), and consistency with prior data releases.
- **Preparing Data:** Usually some data modification is needed before it is shared. For any data that will be shared outside the Agency of origin, data preparation will include the removal of all identifying and confidential information. In addition, case filtering, data element selection or other preparation may be needed prior to data release. This is often the case when preparing data for reports or for use by analysts that are focusing on specific populations or topics. Data subsets may be extracted according to time period, Agency, Agency type or any other dimension contained within the database.

- **Data Tagging:** Each data release must be accompanied by information describing the data source, time period covered, geographic area covered, and populations included. Also, any known data limitations and any context vital to accurately interpreting the data should be included.

17.) Public Data Releases:

The HMIS Team shall approve or deny the general format and content of reports that contain Public Data that will be released. When a report meets the requirements of such a pre-approved format, no further HMIS Team approval is required. However, if a report does not meet such a pre-approved format, HMIS Team's approval shall be required and the HMIS Team shall respond to such requests for Public Data, coordinating efforts and serving as a resource to other staff and providing information to Clients regarding use and disclosure of their Protected Personal Information collected, received, used, or disclosed by the HMIS. If IHCDA administration denies an external party access to the HMIS data or adds unacceptable modifications, that party may petition the IHCDA Data Collection and Evaluation Committee to review and possibly overturn the decision. The Committee's decision shall be in its sole discretion and shall be final. The external party shall have no further right to appeal. The HMIS Team shall ensure that HMIS Staff maintains a log of the dates and content of any reports of Public Data that are generated and released.

- **Certify Readiness:** The HMIS Team must approve every data or report release and must determine that the data is statistically valid for sharing. There is no one standard test; it is a judgment call made by professionally trained database specialists under management of or contracted by IHCDA. However, one statistical test might be sufficient coverage of the data subsets involved (*e.g.*, at least 60% of all data parameters). The data must meet Minimum Necessary level either pre-determined by formal thresholds or established based on the HMIS Team's judgment or by the judgment of a professional data analyst hired for the purpose of certifying HMIS data. If Public Data is to be released that is not statistically valid, appropriate caveats and context must be attached to the data.
- **Types of Public Information Released:** There are several types of Public Data that may be released. Information that may be released is Aggregated Data and some Client-level De-identified Information.
    - **Pre-set Summary Reports** – simple reports of predefined information and timing released to agencies, funders' analysts, and other Stakeholders.
    - **Required Reports** – including the Annual Performance Report (APR) for the U.S. Department of Housing and Urban Development and other agreed upon reports required by local funders, county, state, and federal organizations.

- **Ad-Hoc Reports** – including HMIS-generated reports such as "Community Snapshots," progress reports, average length of stay reports.
- **Participation Reports** The following shall apply to Participation Reports:
    - IHCDA will use the Housing Inventory Chart of the Continuum of Care ("CoC") in Indiana to determine the number of Emergency Shelters, Transitional Housing, and Permanent Supportive Housing programs in each CoC Region.
    - IHCDA will publish lists of programs that are participating in the HMIS and distribute the list to local and regional CoC networks, city leaders, and other key organizations.
- Client Level Data: De-identified Client-level data to be used for subsequent data analysis. Often, the tables are only a selected sample (usually filtered for Client population, time period, and service type or something similar) of the total cases available. Data tables are only available under the following conditions:
    - the users are certified and pre-approved and,
    - a written request to disclose data is submitted and approved by HMIS Team; such requests may be on-going.

  Release Notification: The following actions will be taken whenever HMIS generated data or report is released to the general public or to parties not directly participating in the HMIS, except for Ad-Hoc and Participation Reports as described above.

a. In the case of released reports, identified agencies and programs will be given the opportunity to review and comment on the reports before public release.
b. In the case of released reports, notification will be posted on the IHCDA web site at the time of release.
c. The Data Collection and Evaluation Committee will regularly be given reports summarizing the data access requests and permissions, and the report releases.