Indiana Housing & Community Development Authority

Indiana Balance of State Continuum of Care
Homeless Management Information System (HMIS) Security Plan

All agencies must comply with the current HMIS Privacy, Confidentiality, and Security standards issued in the HUD Notice on 7/31/2004.

- (https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice)

These standards are subject to change during the grant year, but the notice currently requires, but is not limited to:

- Installing virus protection software, with an automatic update on every computer that accesses HMIS
- Utilizing any supported operating system and keep up to date on operating system updates.
- Activating a locking screen saver on every computer that accesses HMIS
- Posting the HMIS Privacy Notice (long version) on its agency website (https://www.in.gov/ihcda/indiana-balance-of-state-continuum-of-care/)
- Installing an individual and/ or network firewall
- Posting "Privacy Notice" signs at each intake desk (https://www.in.gov/ihcda/indiana-balance-of-state-continuum-of-care/)

Reporting malware, ransomware, or any other attacks to your internal infrastructure.

Security breaches of your agency must be reported within 24 hours to your respective help desk.

IHCDA staff, and HMIS contractors, will monitor HMIS participation through **periodic desktop and/or onsite** monitoring, in addition to ongoing review of data quality in the HMIS and DV ClientTrack information systems. The Indiana BoS HMIS team requires a self-audit monitoring to be completed by each HMIS and DV ClientTrack participating agency annually. IHCDA will send the survey to Site Administrators of the agency during the grant year/evaluation period. Data will also be reviewed within the monitoring & claims process for HUD sponsored housing programs. IHCDA reserves the right to withhold payment until HMIS violations are corrected or required levels of data quality are achieved. For example, violations include, but are not limited to a percentage of "Missing" or "Don't Know/Refused" responses for universal data elements above 5% for any element.

Agencies must respond to IHCDA in writing when notified of HMIS Policy Violation within **10 business days** of receipt. Agencies should inform IHCDA of their corrective action response to the violation within the 10-business day period following notification by IHCDA. Failure to comply with HMIS requirements may result in IHCDA withholding payments until errors are corrected and compliance with requirement is restored and documented, or termination of the grant(s). 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.

Privacy Policy
IHCDA and the Indiana Balance of State Continuum of Care, will not sell or rent Personally Identifiable Information (PII) that we collect on clients in the information system, and will not collect or share Personally Identifiable Information (PII) absent reasons provided in the Notice of Privacy Practices, referenced in the section entitled "How your information in the HMIS may be used or disclosed: "

Log Files: IHCDA and HMIS contractors may use IP addresses to analyze trends, administer the system and gather broad demographic information for aggregate and metadata use.

All requests for 3rd party system access are referred to the IN 502 CoC Board of Directors for review and decision.

Security Policy
IHCDA and HMIS contractors take every precaution to protect the information of clients. When you submit sensitive information via the HMIS, your information is protected both online and off-line. When HMIS/DV ClientTrack users are asked to enter sensitive information (such as a social security number), that Personally Identifiable Information (PII) is encrypted. While on a secure page, the lock icon on the bottom of web browsers, such as Mozilla Firefox and Google Chrome, become locked, as opposed to unlocked, or open, when you are just 'surfing'. While we use SSL encryption to protect sensitive information online, we also do everything in our power to protect client information off-line. All of our client information, not just the sensitive information mentioned above, is restricted. Only IHCDA and HMIS contractors, and authorized IHCDA staff, who need the information to perform a specific job, are granted access to Personally Identifiable Information (PII). The systems that store Personally Identifiable Information (PII) reside on secure cloud-based servers.

Upon execution of the Participating HMIS Agency Agreement and any use of HMIS/DV ClientTrack information system, the agency agrees to consent to the monitoring of system use and security at all times, whether HUD funded or not. If such monitoring of HMIS/DV ClientTrack information system reveals any possible violations of the law, pertinent information will be provided to law enforcement officials. Any persons using HMIS or DV ClientTrack 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:

A. All HMIS/DV ClientTrack information systems end users
B. Employees of all participating HMIS agencies
C. Participating HMIS agency contractors
D. Partners and Funders
E. Volunteers of participating agencies
F. Indiana Continuum of Care Board of Directors
G. Indiana Housing and Community Development Authority Board of Directors
H. Indiana Housing and Community Development Authority employees, contractors, and vendors
I. Technical assistance providers

IHCDA and HMIS contractors place highest priority on the security of its systems, and the private information they contain. IHCDA and HMIS contractors continually work to protect data and systems:

- Confidentiality
  - Access to client information must be tightly controlled and people with access to confidential information must understand their personal responsibility to maintain its confidentiality.
- Integrity
  - Client information must be protected so that it cannot be modified while in transit or storage. Reported data must be accurate.
- Availability
  - Systems must be available to users when and where they need them. If an employee leaves your agency, Site Administrators must inform IHCDA, via the HMIS or DV Help Desks within one (1) business day, so the user account can be deactivated, and user access removed to system data.

Information Security Procedures:

All IHCDA and HMIS contractors are responsible for protecting the confidentiality and security of HMIS data systems and the human services client information they contain. Information concerning the security related tasks an agency employee is responsible for is included in the employee’s job description. The agency is responsible for ensuring information that is printed from the HMIS is also kept confidential, private, and secure.

For any malware, ransomware, or any other attack on your internal IT infrastructure; those issues must be reported to Grant Peters, HMIS Manager, within 24 hours of system(s) compromise, to your respective help desk. For HMIS, HMIShelpdesk@ihcda.IN.gov, and for DVCT participating agencies, DVhelpdesk@ihcda.IN.gov. The HMIS Manager will work with agency personnel to identify the issue, and establish a corrective action plan to ensure no client data was comprised. The ClientTrack software is a cloud-based web system and non-aggregate client data should never be downloaded to your personal machine. This will alleviate any policy violations in the event of a system attack.

Data Sharing across Providers

At point of service, the client may authorize an agency to access existing information in the HMIS, and to add and update information in the client record to the HMIS. When the client approaches another organization, the authorization process should be repeated. This ensures that no agency accesses a client’s record without that client’s specific permission, and it significantly increases client confidence in the HMIS. The Regional Chairs of the 16 Balance of State regions have signed MOUs that allow for data sharing across agencies, but this is limited to aggregate data.

Data Disposal

Removable drives/devices/laptops/desktops/thumb drives and any other electronic media or equipment will be disposed of by means of physical destruction and/or wiping/magnetization for erasure before disposal. Hard copy info must be shredded or securely deleted from all identifying information.

Coordinated Entry

A client consent will be required as part of the Coordinated Entry process. This will allow all HMIS participating agencies to access client info regardless of agencies HIPAA obligations. At point of service the client may authorize an agency to access existing information in the HMIS, and to add information about the client to the HMIS. When the client approaches another organization, the authorization process is repeated. This ensures that no agency accesses a client’s record without that client’s specific permission, and it significantly increases client confidence in the HMIS. The HMIS systems implied consent policy remains.

“Protected” Information

Protected Agency: Certain agencies that deal substantially with HIV/AIDS, domestic violence, substance abuse, mental illness, or legal services are designated as Protected Class agencies. If your agency is a Protected Class agency, all Client Services Information records (including referrals) are hidden, or protected, from view by any other agency. Basic client information will still be accessible to other agencies.

Access to Data for Monitoring

IHCDA, as the lead HMIS agency, will have limited access to your agency's data for monitoring purposes and aggregate reporting purposes. All IHCDA HMIS staff and HMIS contractors who have access to data will undergo confidentiality and ethics trainings.

Unauthorized Access to the IHCDA system:

Any user accessing the HMIS or DV ClientTrack information systems must be affiliated with a participating HMIS agency, be in good standing, and have an executed User and Agency agreement on file. Additionally, each system end user must attend the required user trainings, and provide a completed User Agreement form in order to be given a User ID and Password. Unauthorized access is prohibited and is grounds for legal action. Users must also attend Security and Confidentiality training in order to remain active users. End users who do not log in to the systems for over 90 days are required to complete security training in order to regain access to the system.

Client Grievances

Documentation of client refusal must be maintained in each client file. Individuals refusing to authorize participation in HMIS should be discussed with the funder /funding stream. An ID number will be assigned to document equivalent HMIS data elements to be gathered and documented in the case file. A client's refusal to participate in HMIS does not allow the agency to deny services to the client, and they may only be available for limited services at your organization for the HUD funding stream.

Grievance Procedure

The client has the right to appeal his or her individual complaints related to their HMIS data to the entering agency in accordance with the agency's established Grievance Policy. Complaints about the conduct or practice of HMIS may be filed electronically or in writing to Grant Peters, HMIS Manager at IHCDA, at HMIS@ihcda.IN.gov. Agencies are responsible for establishing an internal grievance process to handle client complaints and grievances related to consent and release of information related to the HMIS system. If a client has a grievance regarding erroneous data entry, or inappropriate use of their data, they will need to follow the agency's established guidelines, standard operating procedures, or protocol, to resolve these issues.

Revoking Authorization:

The client has the right to revoke their authorization at any time, for any reason.

DEFINITIONS:

- Clients – individuals receiving services from local agencies utilizing HMIS
- User/End User – staff member at local agencies utilizing HMIS
- IHCDA – Indiana Housing and Community Development Authority
- HMIS – Homeless Management Information System