HMIS Standard Operating Procedures and Policies

Approved:
Revised: 5/5/2025

Borrowed from the ihcda, HMIS Standard Operating Procedures

United Caring Services

HMIS SOP's Table of Contents

Introduction

The purpose of this Handbook is to inform employees of the conditions, benefits, and obligations of United Caring Services and its use of HMIS Software.

SECTION 1: GENERAL

1.1 Our History

The United Caring Shelter, Inc., dba United Caring Services (UCS) began in June 1991, formally incorporating in 1993, thanks to the mission-minded willingness of Bethel United Church of Christ's adult Sunday school class under the leadership of Rev. Joe Fraccaro who wanted to serve a meal to homeless and hungry.

- In 1991, UCS opened a day shelter at St. Anthony's Family Life Center. An emergency night shelter for men was then added in an area of Emmanuel Lutheran Church.
- In 1996, UCS bought an abandoned brick warehouse on 6th street close to the main bus terminal and other services. This building on the first floor became the day shelter with the second floor acting as the men's night shelter and administrative office.
- In 2001, construction began on the 3rd and 4th floors to provide apartments first as a transitional housing program for men; then in 2017 as low income, permanent housing for men and women.
- In 2009, UCS partnered with Pigeon Township to start providing White/Red flag emergency shelter services for people during inclement weather.
- In November 2011, UCS opened an emergency night shelter for single women in the former St. Anthony Convent on First Avenue.
- In January 2013, after a merger was formalized, Ruth's House became the women's emergency shelter for UCS.
- In July 2013, United Caring Shelters, Inc. announced that it would rename the organization and do business as United Caring Services stating that this name change reflects the growth of the organization as a community of caring.
- In November 2014, UCS opened the community's first and only homeless medical respite program (HMRP) with 6 beds for men.
- In January 2017, UCS expanded medical respite services by 4 beds to meet the needs of women.
- In 2022 UCS acquired Zion House for shared housing.

1.2 Our Mission Statement, Vision and Values

United Caring Services strives to embody the core values of the organization in its employment relationships, collaborations, and in relationships with its clients. Employees should be guided by the mission, vision and values of UCS in the performance of their duties.

Mission

To provide values-based, low barrier, sustainable, and high-quality homeless shelters, services, and solutions.

Vision

To be a place where individuals, organizations, and agencies collaboratively create a community of caring.

Values

Dignity, Faith, Commitment, Compassion, Integrity, Unconditional Love, Service, Passion

1.3 Diversity, Equity, and Inclusion Statement

United Caring Services seeks to be a community of caring and to promote that ideal throughout our wider community. We value diversity. Our community is stronger, and our decisions are wiser when they are made up of people with different backgrounds, representing a wide range of ideas. We seek to practice equity. We know that "one size doesn't fit all," and so we strive to help both guests and staff get what they need to thrive. We foster inclusivity through our mission, governance, and services. This means that we take affirmative steps to hire, train, and promote qualified people from all segments of society. We collaborate with individuals, agencies, and organizations that embrace and demonstrate these beliefs.

1.4 Equal Employment Opportunity Statement

United Caring Services prohibits discrimination in all of its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex, marital status, familial status, parental status, religion, sexual orientation, political beliefs, genetic information, reprisal, or because all or part of an individual's income is derived from any public assistance program. Should you have concerns, questions, or complaints, please speak with the Director of People and Programs, or the UCS Executive Director.

Nothing written in any United Caring Services policy shall be interpreted to conflict with or to eliminate or modify in any way the employment-at-will relationship. No representative of UCS may modify or enter into any agreement, oral or written, which changes the at-will relationship. Management should not make any representations to employees or applicants concerning the terms or conditions of employment with UCS that are not consistent with this policy.

SECTION 2: HMIS Overview

2.1 Overview

A Homeless Management System (HMIS) is a local information technology system used to collect client-level data and data on the provision of housing 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, Indiana Housing and Community Development Authority (IHCDA) contracted with ClientTrack, Inc. (Eccovia to provide the HMIS software. The focus of this effort was to expand participation in HMIS homeless service providers. In 2013, IHCDA established a closed database, that is comparable to the HMIS database, to victim service providers, known as the Domestic Violence (DV) ClientTrack production system. IHCDA allows agencies located in the Indiana Balance of State, and provides services to the people experiencing homelessness, to participate in the HMIS and DV production systems at no charge.

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 reviews 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.

2.2 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 (Such as United Caring Services), the HMIS Software Vendor, and any other entity involved in the administration of the Indiana BoS HMIS. This includes all employees of United Caring Services that have direct access to the HMIS system, and all members who have access to and use of the intake and discharge forms.

2.3 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 "Site Administration and Enforcement of Policy."

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

Client: A person who applies for or receives services from an Agency such as United Caring Services.

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.

HIPPA: 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 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 (United Caring Services) 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 protected 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.

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

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 Dara Standards are effective October 1, 2021.

2022 HUD Data Standards Universal Data Elements

- Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- 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

SECTION 3: Site Administration and Enforcement of Policy

3.1 Identification of Site Administrator and Deputy Site Administrator

Site Administrator/Deputy Site Administrator

- The Site Administrator shall be the Executive Director
- The Deputy Site Administrator shall be the Director of Programming
- The Site Administrator and the Deputy Site Administrator shall share responsibility for the following.
    - Each Agency must identify an individual who will serve as its Site Administrator, for setting up new user accounts and serving as a point of contact for data quality issues and corrections. Site Administrators are responsible for protecting HMIS data. Time, interest, and ability are the biggest factors for determining who should be a Site Administrator for HMIS. The Site Administrator must have an active HMIS or DV production system 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 United Caring Services User, who has been vetted by the Site Administrator and applicable pre-employment background checks as conducted by the Site Administrator Agency. Access to HMIS/DV ClientTrack should be based on each United Caring Services User's job function/descriptions as it will relate to the HMIS and DV production systems data entry and retrieval (i.e., role-based security).
    - Detecting and responding of security violations, and data quality errors of HMIS policies or United Caring Services policies and procedures.
    - In conjunction with IHCDA, decisions regarding the issuing, altering, and revoking of HMIS access privileges.
    - Ensuring system auditing (within United Caring Services) 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 United Caring Services individual(s) for working with United Caring Services end users to correct data quality errors.
    - Ensuring data quality.
    - Ensuring the security of the HMIS on the United Caring Services website and

network.
- Notifying IHCDA staff of any security breach within twenty-four (24) hours of the breach.
- Enforcing United Caring Services information system policies and standards.

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

3.3 Enforcement of Proper Use of the HMIS:
All United Caring Services Users must sign the **HMIS User Agreement/Code of Ethics for HMIS Providers or the ClientTrack 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 United Caring Services 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 United Caring Services Users' employment, and could result in disciplinary action, up to and including termination of Users employment with United Caring Services or affiliation with HMIS as well as potential personal civil and criminal legal fines and penalties.

3.4 User Access Privileges to HMIS:
United Caring Services User access and access levels may be determined by the Executive Director and the Director of Programing in consultation with the IHCDA HMIS Manager. HMIS Staff will generate a username and password for each United Caring Services User, who will be required to generate a unique password his or her first time accessing the HMIS. Each individual user should be the only person who will know his or her unique password.

3.5 United Caring Service HMIS 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 United Caring Services when taking on a position that will require use of the HMIS system.
- United Caring 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 the same. All United Caring Users have a critical role in the effort to protect and maintain Client information contained in the HMIS.
- 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 workstations 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 Personal Protected Information (PPI) that have been collected or for which Agency Users have been given access privileges.
- Accept responsibility for all activities associated with the use of their United Caring Service accounts and related access privileges.

3.6 Implementation Assessments:
United Caring Service consents that they 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.

3.7 Password:
- United Caring Services only permits access to HMIS with use of a user authentication system consisting of a username and password which the User may not share with others. Temporary passwords are created when a new User is created.
- The 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 Users cannot share passwords and passwords should be stored securely and not be accessible to other people. Passwords should never be stored or displayed in any publicly accessible location. Passwords should be designed to prevent any User from being able to log onto more than one (1) workstation at a time, and to prevent any 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 (alphanumerical). Passwords should not use or include the User's username, the HMIS name, or the HMIS Software Vendor's Name. Passwords should be easily guessed or consist entirely of any common word found in any dictionary (spelled in correct or reverse order).
- Passwords should be changed periodically by each User. IHCDA requires that HMIS passwords are changed at least every ninety (90) days.
- The Agency Site Administrator must immediately notify IHCDA staff of any User's termination to allow IHCDA staff to terminate the 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 (30) days of inactivity.

SECTION 4: Security

4.1 General Security Protocols:
United Caring Services has the following general security protocols that staff, volunteers, and administration must follow.

- 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. Regarding raw data: United Caring Services 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 raw format of a United Caring Services computer, this data becomes the responsibility of United Caring Services.

- All downloaded Client level data from the HMIS must be saved in a private, not shared folder, where only the User who downloaded the data can access it. All downloads should only happen on computing systems in which the computing system is only accessible via that Users username and password.
- **All Client level data that is printed or gathered via a hardcopy form, must be stored in a locking drawer, in an office that locks and is only accessible via staff.**
- All User computers, when not in use, must be locked, and if in an office, the door closed and locked.
- UNDER NO CIRCUMSTANCES SHOULD CLIENT LEVEL DATA BE LEFT IN AN OPEN AND ACCESSIBLE AREA FOR EASY VIEWING.
- Client level data should never be accessed from outside of the office and during working hours. Violation of this may be considered a violation of United Caring Services User's employment, and could result in disciplinary action, up to and including termination of Users employment with United Caring Services.
- The HMIS is a secure database which allows twenty-four (24) hour access to all qualified Users.
- The HMIS software will automatically log off after a pre-set interval of inactivity.
- The use of HMIS always constitutes 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 person using HMIS or information obtained for this application without proper authorization or in violation of these policies and procedures may be sub to civil and/or criminal prosecution. Any person enabling access by an unauthorized individual may also be subject to internal disciplinary actions in addition to civil and/or criminal prosecution.
- Client information must be protected so that IT cannot be modified. Reported data must be accurate.
- Users must not transmit Client Level Data over public networks. Users must use the following procedures.
    - Data extracted from the HMIS should be stored locally and not on a public or open network.
    - 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 question should be directed to the Executive Director or the Director of Programming with United Caring Services.

4.2 Media and Hard Copy Protection:

It is the responsibility of United Caring Services and its employees to secure any electronic media or hard copy containing identifying information that is generated either by or for HMIS, including, but not limited to, 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 staff are not present, the information must be secured in areas that are not publicly accessible in a secure manner (e.g., a locked filing cabinet or locked office).

- All hard copies are to be only stored for the time of the clients stay in the programming of United Caring Services and **disposed of after one month of their departure**.
- All documents for disposal are to be placed in the locked shredding box, and the actual disposal will happen by Piranha Shredding and Recycling or contracted to another company who does the same.

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

Any staff volunteer or other person who has been granted a User ID and password and 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 User may be subject to discipline by United Caring Services pursuant to the United Caring Services Employee Handbook.

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. United Caring Services serves these protected classes of clients, and may hide the Client's case notes, diagnoses, and treatment from other agencies using HMIS. In the event of a request for PPI by another agency, United Caring Services has the right to seek its own legal advice.

4.4 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 a User and access activity and for the possible creation of historical logs and access violation reports. The Executive Director and/or the Director of Programming 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 inappropriate access.

4.5 Computer Operating System Maintenance:
United Caring Services will keep all computing systems updated with the latest security and other updates recommended for the operating system. The local and server network computers will have automatic updates on every computer that accesses HMIS.

4.6 Firewall and Virus Protection:
United Caring Services will 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.

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 as 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 United Caring Services Users on the system where the HMIS application is housed. The virus software must have automatic updates or regularly updated.

SECTION 5: Security Violations

- All security breaches must be reported first to the Executive Director and/or the Director of Programming immediately. Then the Executive Director will report the breach to the HMIS Team within twenty-four (24) hours.
- 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 United Caring Services.
- If during the cost of auditing, it is determined that United Caring Services has a HMIS policy or security violation, United Caring Services must respond to IHCDA in writing within TEN (10) working days after being notified of the HMIS Policy Violation (breach in security) or the incident is discovered by United Caring Services. United Caring Services must inform IHCDA of how it has addressed the violation. Failure to comply with HMIS requirement 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 United Caring Services being ineligible for funding or receiving a low HMIS performance score in the next year.

SECTION 6: 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 security reviews to provide United Caring Services with expectations for monitoring. The goal of the audits is to ensure that United Caring Services is complying with security requirements. IHCDA will work with United Caring Services if it receives findings to ensure they are remedied as quickly as possible.
- **Consequences of Security Violation**s:
    - First time offense – Findings will be assessed for the security breach. These

issues must be resolved by the date specified by IHCDA. United Caring Services may be warned and/or additional training may be required.
- Second time offense – United Caring Services access to HMIS may be suspended, points may be taken away from current or future funding applications, or United Caring Services may be required to assign the right of use/enter their client's information to another individual or entity.

SECTION 7: Implementation Assessments and Denial of User or Participating Access

United Caring Services is responsible for understanding and ensuring that our 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

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

United Caring Services 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 are not specific to the HMIS.

- IHCDA shall call the Executive Director or the Director of Programming if the Executive Director is not available, to arrange a time to meet.
- Violations of security or privacy protocols will be investigated by United Caring Services and HMIS Staff.
- All confirmed violations of a breach of a Client's PPI will be communicated in writing by United Caring Services 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 United Caring Services and sent to IHCDA and place in the Sent file at the Agency.
- If United Caring Services 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 United Caring Services User found to be in violation of security protocols may be sanctioned accordingly. Sanctions may include but

are not limited to: (i) submission of a plan of correction, (ii) a formal letter of reprimand, (iii) suspension of HMIS privileges, (iv) revocation of HMIS privileges, (v) termination of the HMIS Participation Agreement, (vi) 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 actions for violation of the procedures described herein even if the violation is discovered by IHCDSA through other means.

SECTION 8: HMIS Training

All United Caring Services Staff who have HMIS access will be required to attend HMIS training hosted by HMIS Staff, bi-annually. Confirmation of the training will be done through a verified registration for said training and attendance at a scheduled webinar training, or in person training hosed 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 the training will be evidenced by the attendance reports maintained for online webinars and/or sign-in sheets at live training courses. Any United Caring Services User found to be logging in to training but not actively following the session, as evidenced by electronic monitoring of alternate keystroke activity, failure to connect and other open windows, will be required to repeat the training.

SECTION 9: HMIS Technology Requests

United Caring Services must complete and submit technology requests via email.

- 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, United Caring Services 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.

SECTION 10: Data Use and Disclosure

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

- United Caring Services Users: Users are responsible for ensuring that all Client information is fully protected, and that all data use conforms to IHCDA adopted policies.
- United Caring Services and Programs: The **HMIS Participation Agreement** must be signed, (posted on **Indiana Balance of State Continuum of Care – HMIS and DV ClientTrack**) pledging our agreement and support of all policies. Agencies also agree to post the **HMIS Statement of Privacy Practices** that defines the right of Clients.

10.1 Disclosures and Allowable uses of Protected Personal Information:

- 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 to 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 the 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 and in consultation with IHCDA:

- **10.2 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.
- **10.3 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 reasonable able to prevent or lessen the threat. Including the target of the threat.
- **10.4 Uses and Disclosures about Victims of Abuse, Neglect, or Domestic Violence:** PPI about an individual who United Caring 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 statue or regulation; and United Caring Services believe 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 of the United Caring Services, in the exercise of professional

judgement, 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 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, in the exercise of professional judgement.

- **10.5 Uses and Disclosures for Academic Research Purposes:** PPI may be used and disclosed for academic research purposes conducted by an individual or institution that has a formal relationship with IHCDA if the research is conducted either:
    - By and 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 Executive Director or, in unavailable, the Director of Programming.
    - All Uses and disclosures for Research purposes shall comply with the ("IHCDA HMIS Research Policy"). Further a written 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 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 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.
- **10.6 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: (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.

- 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.

SECTION 11: Client Grievance Policy

Client Grievance Policy:
If any Client wishes to file a grievance about the collection, handling, or disclosure of any Client Level Data or Personal Protected Information (PPI), they must submit the grievance in writing to the Director of Programming so that it may be recorded and added to their file. Each grievance will be handled on a case-by-case basis, with varying outcomes based on the situation.

SECTION 12: User Responsibilities

- Users must be prepared to answer Client questions regarding the HMIS.
- Users must respect Client preferences with regard to the entry and sharing of PPI within the HMIS. Users must accurately record Client's preferences by making the proper designations as to sharing of PPI and/or any restrictions on the sharing of PPI.
- Users must allow a Client to change his or her information sharing preferences at the Client's request (i.e., to revoke consent).
- Users must not decline services to a Client or potential Client if that person:
    - refuses to allow entry of information into HMIS (except if the information is required to determine eligibility for housing or services or to assess

needed services, or if the information is required to be collected as a condition of a provider agreement).
    - refuses to share his or her personal information with other service providers via HMIS.
- The User has primary responsibility for the information entered by the User. The information must be truthful, accurate, complete, and timely to the best of User's knowledge.
- The User will enter information into the HMIS database on a regular and consistent basis. "Regular and consistent" means within a five (5) business day period of intake or discharge. Annual update of a Client's status is also required.
- Users will not solicit from or enter information about Clients into the HMIS unless the information is required for a legitimate business purpose approved by the Agency such as to provide services to the Client. Users must enter information into the HMIS database only with respect to individuals which the Participating Agency serves or intends to serve, including through referrals.
- Users will not alter or overwrite information entered by an agency other than their Participating Agency.
- Users will not include profanity or offensive language in the HMIS; nor will Users use the HMIS database, in violation of any law or to defraud any entity or to conduct any illegal or unauthorized activity.

SECTION 13: Documentation of Homelessness

Maintaining documentation of each participants' homeless status is an extremely important aspect of ESG project management. ESG sub-recipients are required to obtain and maintain adequate documentation of the evidence used by the sub-recipient to establish and verify the homeless status of persons being served. Written, dated and signed documentation of homeless status must be maintained in each participant's file.

The order of preference for documentation to demonstrate homelessness status is as follows:

1. Third-party documentation (obtained from another service provider or third-party who is aware of the household's living situation.)
2. Intake worker observations
3. Self-declaration

When third-party or intake worker observation documentation is not obtainable sub-recipient must provide a record of due-diligence and the steps that were taken in attempting to obtain that level of verification. Maintain the record of due-diligence with the self-declaration form in the participant file.

Lack of third-party documentation must not prevent the household from being immediately admitted to an emergency shelter, receiving street outreach services or receiving services provided by a victim service provider.

If the Head of Household is unable to provide a written self-declaration the sub-recipient staff member is encouraged to write down the Head of Household's personal account and document it on the form.

The Participant Eligibility Worksheet (HUD Homeless Documentation form) was created for use as a guide for proper documentation of homelessness. This is the form that UCS will use to provide documentation of homelessness. The Participant Eligibility Worksheet (HUD homeless documentation form) can be found on IHCDA's ESG Web site: http://www.in.gov/myihcda/2450.htm.

HUD has clarified the definition of homeless and the ESG program recognizes the following characteristics as being eligible for participation in the ESG program:

- An individual or family who lacks a fixed, regular, and adequate nighttime residence, meaning:
    - Has a primary nighttime residence that is a public or private place not meant for human habitation;
    - Is living in a publicly or privately operated shelter designated to provide temporary living arrangements (including congregate shelters, transitional housing, and hotels and motels paid for by charitable organizations or by federal, state and local government program); or
    - Is exiting an institution where (s) he has resided for 90 days or less and who resided in an emergency shelter or place not meant for human habitation immediately before entering that institution.
- An individual or family who will imminently lose their primary nighttime residence, provided that:
    - Residence will be lost within 14 days of the date of application for homeless assistance;
    - No subsequent residence has been identified; and
    - The individual or family lacks the resources or support networks needed to obtain other permanent housing.
- Any individual or family who:
    - Is fleeing, or is attempting to flee, domestic violence, dating violence, sexual assault, stalking, or other dangerous or life-threatening conditions that related to violence against the individual or family member, including a child, that has either taken place within the individual's or family's primary nighttime residence or has made the individual or family afraid to return to their primary nighttime residence;
    - Has no other residence; and
    - Lacks the resources or support networks e.g., family, friends, faith-based or other social networks, to obtain other permanent housing

SECTION 14: Maintenance of Records.

The Subrecipient shall maintain all books, records, documents, and other evidence pertaining to the Project and all costs and expenses incurred and revenues received under this Agreement in sufficient detail to reflect all activities undertaken in connection with the Project and all costs, direct and indirect, of labor, materials, equipment, supplies, services, and other costs of whatever nature, for which reimbursement is requested under this Agreement. Such records shall be maintained for a period of five (5) years after the date on which this Award is closed. Records shall be retained beyond the prescribed period if any litigation, claim, negotiation, audit, or another similar type of action to the

foregoing has commenced involving this Agreement, the Award, or the Project. In that instance, the records shall be retained until the litigation, claim, negotiation, audit, or other action has been resolved.

SECTION 15: Appendix

Homeless Management Information System (HMIS) Notice of Privacy Practices Effective 10/2022 Version 4.0

The purpose of this notice is to explain to you why we collect personal information from you and refer you to the HMIS Statement of Privacy Practices for additional information regarding how this information may be used or disclosed. When you request services from this agency, we enter information about you, and members of your family, into a computer system, called the Homeless Management Information System (HMIS). We collect personal information directly from you for reasons that are discussed in our HMIS Statement of Privacy Practices. We may be required to collect some personal information as required by the United States Dept of Housing and Urban Development (HUD), by law, or by organizations that this agency funds to operate this program. The personal information we collect is important to run our programs, to improve services for homeless, or those at risk of homelessness, individuals and families. We may use or disclose your information to provide you with services. We may also use or disclose your information to comply with legal and other obligations. We assume that you agree to allow us to collect information, and to use or disclose it, as described in the HMIS Statement of Privacy Practices. You can inspect personal information about you that we maintain, as provided in the HMIS Statement of Privacy Practices. You can also ask us to correct inaccurate or incomplete information. Please contact the Case Manager, agency Site Administrator, or Executive Director of the agency who entered the data to make this request. Please read the HMIS Statement of Privacy Practices for additional information. You will be provided with a copy of the HMIS Statement of Privacy Practices upon request. HMIS STATEMENT OF PRIVACY PRACTICES Effective: 10/2022 THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. IHCDA's Homeless Management Information System (HMIS) When you request services from this agency, we will enter information about you and your family into the Homeless Management Information System, a computer database commonly referred to as "HMIS". This HMIS is administered by the Indiana Housing and Community Development Authority ("IHCDA"). The HMIS is used by many agencies throughout the state of Indiana that provide services to persons and families in need. The information collected in the HMIS will help us reduce duplicate intakes, document the need for services, provide historical information, and generate reports in order to comply with federal requirements and expectations. How your information in the HMIS may be used or disclosed Unless restricted by other laws, your information will be used as follows: • to provide individual case management, services, and/or treatment to you at this agency and other agencies that use the HMIS • for statistical purposes, such as determining the number of persons that are homeless • to track individual program-level outcomes • to identify unfilled service needs and plan for the provision of new services • to obtain payment for services provided to you • for quality assessment, training, evaluation, legal and business planning, and other health care operations • to allocate resources among agencies engaged in the provision of services • other uses allowed by law The information about you can also be used by, or disclosed to, the following: • Authorized individuals who work for an agency for administrative purposes related to

providing services to you or your family, or for billing or funding purposes. • Auditors or others who review the work of an agency or need to review the information to provide services to an agency. • The HMIS team at IHCDA and its designees, the HMIS software developer, and other individuals involved in maintaining the HMIS may see the information for administrative purposes (for example, to check data errors). • Individuals performing academic research who have signed a research agreement with this agency or IHCDA. Your name, social security number or other identifying information will not appear in any research report. • This agency, IHCDA, or its vendor may use your information to create reports that have your identifying information removed. • Government or social services agencies that are authorized to receive reports of infectious disease, abuse, neglect, or domestic violence, when such reports are required by law or standards of ethical conduct. • A coroner or medical examiner or funeral director to carry out their duties. • Authorized federal officials for the conduct of certain national security or certain activities associated with the protection of certain elected officials. • Law enforcement officials, but the disclosure must meet the minimum standards necessary for the immediate purpose and not disclose information about other individuals. A court order or search warrant may be required. • Others, to the extent that the law specifically requires such use or disclosure. • To others to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, if the disclosure is made to a person or persons reasonably able to prevent or lessen the threat of harm, including the target of a threat. • Other uses and disclosures of your information will be made only with your written consent. You may revoke your consent at any time in writing, except if the agency has already released information, because of your consent. Your rights regarding your information in the HMIS: • You have the right to inspect and obtain a copy of your own Protected Personal Information (PPI) for as long as it is kept in the HMIS, except for: o Information compiled in reasonable anticipation of litigation or comparable proceedings o Information about another individual (other than a health care or homeless provider) o Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information o Information, the disclosure of which would be reasonably likely to endanger the life, or physical safety, of any individual • You have the right to request that your Protected Personal Information (PPI) is corrected when the information in the record is inaccurate or incomplete. • You have a right to request that your personal information be provided to you by alternative means,, or at alternate locations (such as at your home or place of work). This agency will accommodate reasonable requests. • You have the right to receive a list of disclosures of your Protected Personal Information (PPI) made by this agency during the six (6) years prior to the date you request this information, except for disclosures for national security or intelligence purposes or to correctional institutions or law enforcement officials. If a law enforcement official or health oversight agency requests that we temporarily suspend giving you an accounting of disclosures made to them, the request must be time-limited and given to us in writing. Exercising your rights regarding your information in the HMIS You can exercise these rights by making a written request to this agency, or by making a written request to IHCDA. The addresses are listed at the end of this notice. Enforcement of your privacy rights: If you believe your privacy rights have been violated, you may send a written complaint to this agency. If your complaint is not resolved to your satisfaction, you may send your written complaint to IHCDA. Addresses are listed at the end of this notice. You will not be retaliated against for filing a complaint. This agency is required by law to maintain the privacy of your Protected Personal Information (PPI), and to display a copy of the most recent HMIS

Notice of Privacy Practice ("Notice"). This Agency reserves the right to change this Notice from time to time, and if it does, the change will affect all the information in the HMIS, not just the information entered after the change. The revised Notice will be posted by this Agency. You may request a copy of it from this Agency or IHCDA.

UNITED CARING SERVICES, 324 NW 6TH ST, EVANSVILLE, INDIANA 47708
Agency Name: United Caring Services
Telephone: 812.422.0297
Email: driector@unitedcaringservices.org

INDIANA HOUSING AND COMMUNITY DEVELOPMENT AUTHORITY 30 S. Meridian St., Suite 900 Indianapolis, IN 46204 Attn: Grant O. Peters, HMIS Manager
Re: HMIS Protected Personal Information (PPI)

Sistema de Información para la Gestión de Personas sin Hogar (HMIS) Declaración de Prácticas de Privacidad Vigente a partir de octubre del 2023 Versión 5.0

El propósito de este aviso es explicarle por qué recopilamos sus datos personales y le remitimos al Declaración de Prácticas de Privacidad de HMIS para obtener información adicional sobre cómo esta información puede ser utilizada o divulgada. Cuando usted solicita servicios de esta agencia, nosotros ingresamos información sobre usted, y miembros de su familia, en un sistema informático, llamado Sistema de Información para la Gestión de Personas sin Hogar (HMIS). Recopilamos información personal directamente de usted por razones que se describen en nuestra Declaración de privacidad de HMIS Prácticas. Es posible que se nos solicite que recopilemos cierta información personal según sea necesario por el Departamento de Vivienda y Desarrollo Urbano de los Estados Unidos (HUD, por sus siglas en inglés), por ley, o por organizaciones a las que esta agencia financia para operar este programa. La información que recopilamos es importante para ejecutar nuestros programas, para mejorar los servicios personas sin hogar, o en riesgo de quedarse sin hogar, ya sean individuos o familias. Es posible que usemos o divulgamos su información para brindarle servicios. Es posible que también usemos o divulguemos su información para cumplir con las obligaciones legales y de otro tipo. Asumimos que usted está de acuerdo en permitirnos recopilar su información y usarla o divulgarla, como se describe en la Declaración de Prácticas de Privacidad de HMIS. Usted puede inspeccionar la información personal que mantenemos sobre usted, según lo dispuesto en la Declaración de Prácticas de Privacidad de HMIS. También puede pedirnos que corrijamos errores o información incompleta si existen. Para esto, por favor, póngase en contacto con el Administrador de Casos, director ejecutivo u otra persona adecuada de la agencia que ingresó los datos para esta solicitud. Por favor, lea la Declaración de Prácticas de Privacidad de HMIS para obtener información adicional. Se le proporcionará una copia de la Declaración de Prácticas de Privacidad de HMIS si usted lo solicita. DECLARACIÓN DE PRÁCTICAS DE PRIVACIDAD DE HMIS Vigente a partir de octubre del 2023 {00047818-2} ESTE AVISO DESCRIBE CÓMO SE PUEDE USAR LA INFORMACIÓN SOBRE USTED Y DIVULGADA Y CÓMO PUEDE OBTENER ACCESO A ESTA INFORMACIÓN. POR FAVOR REVÍSELO CUIDADOSAMENTE. El Sistema de Información para la Gestión de Personas sin Hogar (HMIS) de la Autoridad de Vivienda y Desarrollo Comunitario de Indiana Cuando solicite servicios de esta agencia, ingresaremos información sobre usted y su familia en el Sistema

de Información para la Gestión de Personas sin Hogar, una base de datos informática comúnmente conocida como "HMIS". Éste HMIS es administrado por la Autoridad de Vivienda y Desarrollo Comunitario de Indiana ("IHCDA"). El HMIS es utilizado por muchas agencias en todo el estado de Indiana que brindan servicios a personas y familias necesitadas. La información recopilada en el HMIS nos ayudará a reducir las ingestas duplicadas, documentar la necesidad de servicios, proporcionar información histórica, y generar reportes a fin de cumplir con requerimientos y expectativas federales. Cómo su información puede ser usada o divulgada en HMIS A menos que otras leyes lo restrinjan, su información se utilizará de la siguiente manera: • para proporcionarle administración de casos individuales, servicios y/o tratamiento en esta agencia y otras agencias que utilizan el HMIS • con fines estadísticos, como determinar el número de personas sin hogar • para realizar un seguimiento de los resultados individuales a nivel de programa • para identificar necesidades de servicios no cubiertas y planificar la prestación de nuevos servicios • para obtener el pago por los servicios prestados a usted • para evaluar la calidad, capacitación, evaluación, planificación legal y comercial, y otras operaciones del cuidado de la salud • para asignar recursos entre las agencias involucradas en la prestación de servicios • otros usos permitidos por la ley La información sobre usted también puede ser utilizada o divulgada a: {00047818-2} • Personas autorizadas que trabajan para una agencia con fines administrativos relacionados con la prestación de servicios para usted o su familia, o para fines de facturación o financiación. • Auditores u otras personas que revisan el trabajo de una agencia o necesitan revisar la información para prestar servicios a una agencia. • El equipo HMIS en IHCDA y sus designados, el desarrollador de software HMIS y otras personas involucradas en el mantenimiento del HMIS pueden ver la información para fines administrativos (por ejemplo, para comprobar errores en los datos). • Personas que realicen investigaciones académicas y hayan firmado un acuerdo de investigación con esta agencia o IHCDA. Su nombre, número de seguro social u otra información de identificación no aparecerá en ningún informe de investigación. • Esta agencia, IHCDA o su proveedor pueden usar su información para crear informes que tengan su información de identificación eliminada. • Agencias gubernamentales o de servicios sociales que están autorizadas a recibir informes de enfermedades infecciosas, abuso, negligencia o violencia doméstica, cuando dichos informes sean requeridos por la ley o las normas de conducta ética. • Un médico legista o médico forense para el desempeño de sus funciones • funcionarios federales autorizados para la realización de determinadas actividades de seguridad nacional o determinadas actividades asociadas con la protección de ciertos funcionarios electos. • funcionarios encargados de hacer cumplir la ley, cuya divulgación debe cumplir con los estándares mínimos necesarios para el propósito inmediato y no revelar información sobre otros individuos. Es posible que se requiera una orden judicial. • Otros, en la medida en que la ley requiera específicamente dicho uso o divulgación. •tros para prevenir o disminuir una amenaza grave e inminente a la salud o a la seguridad de una persona o del público, si es que la divulgación se hace a una persona o personas razonablemente capaces de prevenir o disminuir la amenaza de daño, incluyendo al objeto el objetivo de una amenaza. • Otros usos y divulgaciones de su información se realizarán únicamente con su consentimiento por escrito. Usted puede revocar su consentimiento en cualquier momento por escrito, excepto si la agencia ya ha liberado información, gracias a su consentimiento. Sus derechos con respecto a su información en el HMIS: • Tiene derecho a inspeccionar y a obtener una copia de su propia Información personal protegida (PPI) durante el tiempo que se mantenga en el HMIS, excepto en casos donde: o La información es recopilada con anticipación razonable a litigios o procedimientos comparables. {00047818-2} o La información es sobre otra

persona (exceptuando a proveedores de atención médica o proveedores de servicios para personas sin hogar) o La información en su registro ha sido obtenida bajo una promesa de confidencialidad (exceptuando una promesa de confidencialidad de parte de un proveedor de atención médica o proveedor de servicios para personas sin hogar) y si la divulgación de tal información fuera a revelarla fuente de dicha información o información cuya divulgación podría razonablemente poner en peligro la vida, o seguridad física, de cualquier individuo. • Usted tiene derecho a solicitar que su Información Personal Protegida (PPI) sea corregida cuando tal información en el registro sea inexacta o incompleta • Tiene derecho a solicitar que su información personal le sea proporcionada por medios alternativos o en lugares alternativos (como en su casa o lugar de trabajo). Esta agencia atenderá solicitudes razonables. • Tiene derecho a recibir una lista de divulgaciones de su información personal protegida (PPI) realizada por esta agencia durante los seis (6) años anteriores a la fecha en que usted solicita esta información, excepto para divulgaciones con fines de seguridad o inteligencia nacional o a instituciones correccionales o a la ley funcionarios encargados de hacer cumplir la ley. Si un funcionario encargado de hacer cumplir la ley o una agencia de supervisión de la salud solicita suspender temporalmente darle un informe de las divulgaciones hechas a ellos, la solicitud debe ser por un tiempo limitado y entregado a la agencia por escrito Ejercicio de sus derechos respecto de su información en el HMIS Puede ejercer estos derechos realizando una solicitud por escrito a esta agencia, o realizando una solicitud por escrito a IHCDA. Las direcciones se enumeran al final de este aviso. Aplicación de sus derechos de privacidad: Si cree que se han violado sus derechos de privacidad, puede enviar una queja por escrito a esta agencia. Si su queja no se resuelve a su satisfacción, puede enviar su queja por escrito a IHCDA. Las direcciones se enumeran al final de este aviso. No sufrirá represalias por presentar una queja. Esta agencia está obligada por ley a mantener la privacidad de su información personal protegida (PPI), y mostrar una copia {00047818-2} del Aviso de prácticas de privacidad de HMIS más reciente (“Aviso”). Esta Agencia se reserva el derecho a cambiar este Aviso de vez en cuando y, si lo hace, el cambio afectará toda la información en el HMIS, no solo la información ingresada después del cambio. El Aviso revisado será publicado por este Agencia. Puede solicitar una copia de este a esta Agencia o a IHCDA.

UNITED CARING SERVICES, 324 NW 6TH ST, EVANSVILLE, INDIANA 47708
Nombre de agencia: United Caring Services
Teléfono: 812.422.0297
Correo electrónico: director@unitedcaringservices.org

AUTORIDAD DE VIVIENDA Y DESARROLLO COMUNITARIO DE INDIANA 30 S. Meridian St., Suite 900 Indianápolis, IN 46204 A la atención de: Gerente de HMIS
Re: Información personal protegida de HMIS (PPI)

HMIS User Agreement Code of Ethics for HMIS Providers

This can be attained at: https://www.in.gov/ihcda/files/HMIS-User-Agreement-2024.pdf