Long Island Homeless Management Information System

Policies and Procedures

2024

Long Island Coalition for the Homeless, Inc.
600 Albany Avenue
Amityville, NY 11701
(631) 464-4314 – phone
(631) 464-4319 – fax
www.addressthehomeless.org

Table of Contents

Introduction

The United States Department of Housing and Urban Development (HUD) requires that all recipients of financial assistance under the Continuum of Care (CoC) program, the Emergency Solutions Grant (ESG) program, the Rural Housing Stability Assistance (RHS) program and other programs funded under the McKinney-Vento Act must use a Homeless Management Information System, or HMIS, to collect client-level data on all persons served.

An HMIS is computer software that helps agencies with program administration, operations, and reporting. An HMIS can be used for many different functions including maintaining client and agency information, bed/unit availability, and service delivery. Some of the typical benefits of an HMIS include:

- Improved service delivery and prompt referrals for clients
- Immediate access to important client information
- Quick and easy preparation of reports for funders, stakeholders

Other benefits of an HMIS include the ability to produce unduplicated estimates of the number of homeless persons accessing services from homeless assistance providers, aggregate reporting of basic demographic characteristics of homeless persons and patterns of service use, including information on shelter stays and homelessness episodes over time.

The Long Island HMIS, also known as AWARDS, is a software package developed by Foothold Technology that has been implemented in many communities across New York State and the United States. The Long Island Coalition for the Homeless (LICH), through grants received from HUD, implemented the Long Island HMIS and continues to oversee its strategic direction and administration. LICH, together with the Continuum of Care in Nassau and Suffolk Counties, actively works to increase resource development and quality assurance for the HMIS. LICH staff manage the daily operations of the HMIS, and provide technical support, training, and program customization as needed.

The Long Island Coalition for the Homeless operates in CoC # NY-603.

Service Provider Requirements

Service providers must meet all of the requirements below in order to participate in the HMIS. Failure to develop, implement, maintain or adhere to these policies are grounds for the suspension or termination of an agency's access to the HMIS.

Internal Policy

HMIS participating agencies are required to create and adhere to internal policies regarding each of the following:

1. Each HMIS participating agency must identify an individual whose position includes responsibility for HMIS activities at the agency. This individual will have the full authority to make decisions for the agency regarding HMIS implementation and operation. This person will be assigned as the HMIS Primary Contact and may be assigned to an administrator user group for the HMIS participating agency if a high level of HMIS training is achieved. This person will be referred to as the "Participating Agency HMIS Administrator." Only one person at each agency may be identified as the Participating Agency HMIS Administrator.

2. Each Participating Agency HMIS Administrator must complete the full Foothold approved training for operating AWARDS prior to being issued a user ID and password at that level.

3. An HMIS participating agency shall have access only to data entered by the agency's authorized HMIS users pertaining to clients served by the agency.

4. HMIS participating agencies shall be bound by all restrictions imposed by clients pertaining to the use of personal data that clients do not formally release. It is a client's decision about which information, if any, entered into the HMIS may be shared and with whom. A Client Consent to Exchange of Information shall be signed if the client agrees to share information with any HMIS participating agency other than the agency from which s/he receives services. Currently the NY-603 HMIS does not share client data across agencies.

5. Each authorized HMIS user will be issued a unique user ID and password. Sharing of passwords and user IDs is expressly forbidden. HMIS participating agencies must create and adhere to a policy identifying any violation of the "no-sharing" policy as a serious contravention of agency operations and must further identify appropriate repercussions for such violation.

6. Each authorized HMIS user will complete the full Foothold approved training for operating AWARDS prior to being issued a user ID and password.

User Policy

Each authorized HMIS user will be issued a unique user ID and password. Sharing of passwords and user IDs is expressly forbidden. All HMIS users must take all reasonable precautions to ensure that his/her password is physically secure. Each authorized HMIS user will complete the full Foothold approved training for operating AWARDS prior to being issued a user ID and password.

HMIS users have an obligation to maintain client privacy and to protect and safeguard the confidentiality of each client's protected personal information (PPI). PPI shall include, but not be limited to, the client's name, address, telephone number, social security number, date of birth, type of care provided, medical condition or diagnosis, veteran status, employment information, and any other information relating to the services provided to the client by any agency. Only authorized HMIS users and the client about whom the information pertains may view a client's information in the HMIS. HMIS users must never discuss PPI with anyone in a public area. Information in the HMIS may only be viewed, obtained, disclosed, or otherwise used to enable the authorized HMIS user to successfully perform his/her job.

If client information from the HMIS must be saved in a digital format, then such information must be saved in a secure folder or drive that is accessible only to authorized HMIS users. Hard copies of HMIS data must be kept in a secure file and must not be left in public view. All digital and hard copies of HMIS data will be destroyed when no longer needed.

All authorized HMIS users must log off-of the HMIS prior to leaving the work area where the computer is located. A computer that has the HMIS "open and running" shall never be left unattended for any length of time. Failure to log off-of the HMIS appropriately may result in a breach of client-confidentiality and system security. Authorized HMIS users who notice or suspect a security breach must immediately notify the Participating Agency HMIS Administrator.

Minimum Data Entry

HUD's HMIS Data Standards, as revised October 2017, set forth specific requirements related to client- and program-level data collection and entry in the HMIS. Universal Data Elements must be entered in the HMIS for all persons served, including rostered clients and household members. While the Universal Data Elements are required in accordance with HUD's HMIS Data Standards, entering this information into the HMIS accurately and in a timely manner allows agencies to generate the HUD APR and other reports quickly and with ease.

Recommended Data Entry

The HMIS is a tool to assist agencies in focusing services and locating alternative resources to help homeless persons. Therefore, agency staff should use the client information in the system to target services to the client's needs. Data which may prove to be useful toward this end include:

- Client progress
- Client goals and outcomes
- Supportive and financial services provided
- Referrals

Other data, when entered into the HMIS and reported to a CoC in the aggregate, assist the CoC in applying for and receiving both renewal and new funding from HUD. Such data include:

- Agency program information
- Bed utilization and quarterly occupancy rates
- Data necessary for the annual point-in-time (PIT) homeless count

Goals/Expectations of HMIS Data Completeness

These are aspirational but attainable guidelines for HMIS data entry. Results and success may vary based on project type.

Personally Identifiable Information (PII)	
Data Element	**Error %**
Name	0%
Social Security Number	2%
Date of Birth	2%
Race	2%
Ethnicity	2%
Gender	2%
Universal Data Elements	
Data Element	**Error %**
Veteran Status	3%
Project Start Date	0%
Relationship to Head of Household	3%
Client Location	0%
Disabling Condition	3%
Income and Housing Data Quality	
Data Element	**Error %**
Destination	5%
Income and Sources at Start	4%
Income and Sources at Annual Assessment	4%
Income and Sources at Exit	5%
Timeliness	
Project Start	0-3 Days
Project Exit	0-3 Days

HMIS User Code of Ethics

A. HMIS users must treat all HMIS participating agencies with respect, fairness, and good faith.

B. Each HMIS user should maintain high standards of professional conduct in their capacity as an HMIS user.

C. HMIS users have the responsibility to relate to the clients of all HMIS participating agencies with full professional consideration.

Interview Protocol

Each HMIS participating agency must develop and adhere to an internal interview protocol. This protocol will be integrated into the existing intake procedure. Any additional intake questions are to be asked only for the purpose of data collection or client care.

Additional interview questions will at all times remain consistent with the data elements mandated by HUD. Questions beyond this scope are prohibited.

Privacy/Confidentiality and Security Regulations

HMIS Notice Requirements

HUD has set forth specific guidelines and regulations governing the use of HMIS data, privacy policies and the notification of persons whose personal information may be entered into HMIS. Among the requirements are:

- A "Public Notice" summarizing the HMIS participating agency's HMIS Privacy Policy and purpose of data collection; the Public Notice must be displayed publicly in each office or other location where staff may be collecting personal information about persons, they serve.

- An HMIS participating agency's HMIS Privacy Policy, which must be made available upon request.

Samples of a Public Notice and an HMIS Privacy Policy are attached to this manual (see Attachments A and B, respectively). Please refer to the July 30, 2004, Federal Register for a complete description of the HUD requirements on this topic.

Informed Client Consent

The following is an analysis of New York State and Federal laws that may or may not impact your agency's implementation of the HMIS. It is not exhaustive or necessarily applicable to your agency. It is provided as a courtesy. Agencies concerned about legal implications, as always, should consult their internal general counsel.

Memo prepared for HMIS Committee July 29, 2003 by Victoria Osk of Long Island Legal Services.

INTRODUCTION

This memo provides an overview of the basic laws and regulations governing the types of data and information that will likely be included in the HMIS, based on the types of agencies participating.

The types of data and information that fall under privacy and confidentiality regulations include the following areas: substance abuse; mental health; health care more generally; HIV/AIDS; legal involvement; and social work services.

Each area is governed by its own unique systems of statute and regulation, some state and some Federal, and some of which are somewhat incompatible with others.

SPECIFIC FEDERAL & NY STATE STATUTES AND REGULATIONS

Drug and Alcohol Treatment
Primarily by 42 USC § 290 dd(3) - 290ee(3) and 42 CFR Part 2 (2.3 et seq).

Agencies can share information by executing a Qualified Service Agreement, which is done when one agency consistently provides services to another agency or to their clients. This is typically done when an agency hires a billing service, but can be done for other reasons as well. A client would have the right to know to whom their information might be released pursuant to a QSA. The agency receiving the information pursuant to a QSA would have the same confidentiality responsibilities as the originating program that conveyed the information.

The essential requirement as it relates to the release of specific client information without a QSA in place is that no licensed facility providing treatment can provide information about a client, including the acknowledgment they are a client or have received treatment, without a signed release. The release is mandated by the federal government and requires certain fields of information, including the nature and purpose of the information to be released, specifically to whom it will be released, the dates for which the release period is authorized and the point at which the release expires (which can be either a date or another event), and acknowledgement that the client has been advised of their right not to agree to release the information. There is no general exception for law enforcement, and the information cannot be released pursuant to subpoena, but only in obedience to a court order obtained after notice to the client as well as to the keeper of the records. The holder of the records has the responsibility to defend their privacy in court.

HIV/AIDS
Controlled by Article 27-f of the New York State Public Health Law.

There is no equivalent of a Qualified Service Agreement (QSA) for HIV information; in fact, most state-supervised programs maintaining this information must provide the state with a list of persons within their agency who are permitted access to this information and must regularly train those employees in confidentiality requirements. Every disclosure of HIV information, except for insurance payment, must be noted in the patient's file. A notice prohibiting re-disclosure must accompany HIV/AIDS information release.

Intentional violation is a criminal offense carrying a year in jail, but even inadvertent error, such as mislaying a file containing HIV information, is a violation that can bring civil penalties. As in the case of substance abuse treatment information, no information may be released except pursuant to a state-mandated release, which can be revoked at any time. Only the patient can sign the release unless the patient has been deemed incompetent. In the case of an incompetent person, a legal guardian may sign; incompetence is determined on a case-by-case basis, without regard to age. Therefore, a competent minor has the right to release or to conceal their HIV status, with determination of competence of each minor a rather complex matter entailing an individual evaluation. While there are a number of exceptions to this rule, such as health insurance companies (who have their own confidentiality requirements pertaining to HIV), death certificates, organ donation programs, etc., these are quite limited and specific. As with drug and alcohol programs, the information may not be released in response to a subpoena. Depending on the circumstances, information from which reference to HIV has been redacted may be supplied; if this is not practical, the subpoena must be opposed, and the information released only by court order issued on notice to the patient. There are also state regulations governing the maintenance of HIV information by licensed substance abuse and other state-supervised programs, such as the requirement for special computer security measures.

Mental Health
Section 33.13 or the Mental Hygiene Law of New York State.

Such information is only to be released pursuant to court order, to certain attorney representing the mentally ill, to certain quality control agencies, to certain criminal justice agencies under vary limited circumstances and for the purpose of providing care to the person, or pursuant to a release signed by the patient or a person permitted by law to act on the patient's behalf. Unlike in other instances, however, there are limitations on releases of information based on consent of the patient or their legal guardian; the recipient must have a demonstrable need for the information, and the release of the information must not be detrimental to the patient, requiring some judgment on the part of the agency who has been requested to release information. Other that under those circumstances, agencies governed by 33.13 and its enabling regulations should not even acknowledge their prior contact with a patient. Under certain circumstances, there may be limits placed on the patient's ability to review their own file if such limits are necessary in the patient's best interests, although the patient may contest them.

General Healthcare

In addition to the general demands of doctor-patient privilege, health care providers must comply with the HIPAA privacy rules. All individually identifiable health information is controlled under the HIPAA law. De-identified information, that does not identify an individual, is not controlled by HIPAA.

Entities may share information by executing a Business Associate Agreement (BAA), but these are intended to be limited to those organizations that provide certain services to or on behalf of the covered entity, billing is typical. Such agreements impose strict privacy requirements on the business associate. Patients may review the record sets covered under such agreements.

Under HIPAA, providers must disclose information to patients and to certain federal quality control officers and may (but need not) release the information for certain other purposes, including but not limited to purposes of treatment or payment, public interest or benefits activities (12 areas are designated), and uses and disclosures providing the patient with the opportunity to agree or object, including emergency situations. In that case, fairly informal agreement may be acceptable. However, where HIPAA conflicts with state law, the stricter of the two applies. Where none of the exceptions apply, a detailed authorization must be obtained with various required fields of information. All disclosures must be limited to the minimum necessary. Individuals have a right to an accounting of the disclosure of their information. Individuals may request special restrictions on the use of their information, although the provider may refuse to agree. In general, treatment should not be conditioned on an agreement on the part of a patient to sign an authorization, except in very limited circumstances. Security of electronically maintained information is key to HIPAA, and all providers must have a privacy plan.

Attorney-Client Privilege

All client confidences and secrets must be protected, including, for example, the fact that a client has committed extremely serious crimes, such as homicide. An intention on the part of the client to commit a future crime may be disclosed, but the attorney is not under any obligation to do so. Any violation of this simple rule is considered an ethical lapse that can lead the loss of a license to practice law. If the client is harmed, it is also potential malpractice, entitling the client to possible financial damages. At the same time, the privilege is easily compromised and waived. For example, if an advocate for an agency is present when the client discloses the information, the privilege is waived for all purposes, and everyone present, including the attorney, may be forced to disgorge the information to law enforcement, or in the course of other legal proceedings such as a lawsuit brought against the client.

Minimum Data Element Collection

Each HMIS participating agency agrees to collect and enter in to the HMIS all HUD-required data elements for each person served, including the rostered client and household members (see Universal Data Elements and Program-Specific Data Elements sections). Each HMIS participating agency further agrees to enter in to the HMIS all HUD-required data elements for the agency and its program/s (see Program Descriptor Data Elements section).

Universal Data Elements

Intake date (Project Start date)
Housing Move In Date
Name
Social security number (SSN)
SSN data quality
Date of birth
Birth date data quality
Race
Ethnicity
Gender
Special Needs/Disabling condition
Veteran status
Living Situation prior to program entry
Chronic Homelessness
Destination
Discharge date (program exit date)

Program-Specific Data Elements

Monthly Income and Sources
Non-cash benefits and Sources
Health Insurance
Household Composition
Domestic Violence Victim/Survivor
*Other "funder-specific" information may be required

Program Descriptor Data Elements

Program Name
Program Group
Bed Inventory
Unit Inventory
HMIS Project Type
Funding Source
Operating Start Date
Grant Start Date
Grant ID
CoC #
Intake Form Type
Housing Type
Address
GEO Code
Operational Calendar

LICH will work with Foothold Technology, the AWARDS software developer, to ensure that AWARDS maintains consistency with HUD's requirements. For more information regarding the HUD required data elements and final data standards, please see HUD's Final HMIS Data Standards.

On-Site Equipment

Each HMIS participating agency is required to install and maintain computing resources adequate for accessing the HMIS. The HMIS is web-based software application that requires Internet connectivity. It is **highly** recommended that each participating agency utilize high-speed connections.

Foothold Technology recommends that users access the HMIS from a computer with the following minimum specifications:

- Windows or iOS operating system
- Continuous internet connection
- Current version of either Google Chrome, Internet Explorer, Safari or Firefox

LI HMIS System Administration

LI HMIS Lead

LICH, as the HMIS Lead Entity, will assign administration of the LI HMIS to an LICH employee (the "LI HMIS System Administrator") who shall be responsible for each of the following:

- Provide a single point of communication to all users concerning HMIS issues.
- Communicate system-related changes and information to Participating Agencies.
- Evaluation of requests from HMIS participating agencies for modifications to AWARDS software, and implementation support for HMIS participating agencies.
- Serve as the local HMIS Help Desk providing technical assistance to HMIS participating agencies and users, and problem resolution in collaboration with Foothold Technology.
- Determine training needs, develop training materials, and provide on-going training to Agency Administrators and end users about HMIS data collection, security, and privacy policies and procedures.
- Provide technical support and help develop, troubleshoot, and submit reports such as LSA, SPM, APR, CAPER, NOFA, etc.
- Manage usernames, accounts, and passwords for accessing the HMIS system.
- Monitor compliance with standards of client confidentiality and data collection, entry, and retrieval.
- Participate in HMIS Administrator's training and regular meetings.

The CoC is responsible for the following HMIS functions:

- Designate a single HMIS.
- Select an eligible applicant to manage the CoC's HMIS (called the HMIS Lead).
- Monitor recipient and sub-recipient participation in the HMIS (ensure consistent participation).
- Review, revise, and approve a privacy plan, security plan, and data quality plan for HMIS.
- Ensure that the HMIS is administered in compliance with requirements prescribed by HUD.
- Ensure consistent participation in HMIS of all recipients and subrecipients.

AWARDS Data and Access

The following is a statement from Foothold Technology:

> *Foothold uses two world-class data centers, in two different states, to host our clients' data. These data centers feature uninterruptible power supplies and highly sophisticated disaster prevention and recovery systems. Biometric confirmation of identity is required to enter our data centers. The data centers feature porous floors to prevent flood damage, "dry" sprinkler pipes, fire suppression gas instead of water, a diesel generator that picks up immediately in the advent of a power failure (during the Great Blackout of 2003, our customers (if they had power) were able to use AWARDS with no interruption in service), industrial air filtering and air conditioning technologies and a live 24-hour armed guard.*
>
> *In our data centers, we use servers with multiple hard drives (RAID 5), CPUs, and redundant power supplies so that if any internal components malfunction, there is immediate failover — with minimal interruption in service. Our servers also make use of firewalls in both hardware and software form. We also copy all data to a second server so that if an entire server malfunctions, there is another one ready, again with no service interruption. Lastly, a copy of your data is electronically transferred offsite once a week for safekeeping. No data security and storage procedure is 100% failure proof, but with Foothold, you are able to make use of a continually upgraded, state-of-the-art security program that is well beyond the means of nonprofit agencies acting alone.*

Backup and Disaster Recovery

The backup rotation schedule is currently as follows: all client data is backed up 3 times per day, daily (full day), weekly and monthly. Our disaster recovery plan calls for attempting to recover lost data with as little time lost as possible. Our first attempt will be to use the warm copies that already exist within the same server. If those discs have failed, we will attempt to use the warm copies on our backup server at the same data center. If something has happened to the entire data center, we will utilize a daily backup that resides at our backup data center and if something has happened to both data centers, we will utilize a daily or weekly backup that resides at Foothold Technology headquarters.

System-Wide Access

Access to system-wide client and/or program-level data will be limited to the LI HMIS System Administrator. All other agencies are prohibited from and unable to access system-wide client and/or program-level information.

Attachment A: Sample Public Notice

LICH HMIS Posted Data Privacy Notice

We collect personal information about the people we serve in a computer system called HMIS (Homeless Management Information System). Many social service agencies use this computer system.

We use the personal information to run our programs and to help us improve services. Also, we are required to collect some personal information by organizations that fund our program.

You do not have to give us information. However, without your information we may not be able to help you. Also, we may not be able to get help for you from other agencies.

You have a right to review the personal information that we have about you. If you find mistakes, you can ask us to correct them.

You have a right to file a complaint if you feel that your data privacy rights have been violated. Please tell our staff if you have questions. If you need a grievance form or a complete copy of our privacy policy, please ask our agency staff.

Attachment B: Sample HMIS Privacy Policy

ABC Homeless Organization
Privacy Policy Notice

Brief Summary

This Notice describes the Privacy Policy of the ABC Homeless Organization. We may amend this Privacy Policy at any time. We collect personal information only when appropriate. We may use or disclose your information to provide you with services. We may also use or disclose it 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 this Notice. You can inspect personal information about you that we maintain. You can also ask us to correct inaccurate or incomplete information. You can ask us about our Privacy Policy or practices. We respond to questions and complaints. Read the full Notice for more details. Anyone can have a copy of the full Notice upon request.

ABC Homeless Organization
HMIS Privacy Policy Notice

Full Notice

A. <u>What This Notice Covers</u>

1. This Notice describes the Privacy Policy and practices of ABC Homeless Organization. Our main office is located at 123 Main Street, Anytown, USA, (516) 555-1212.
2. The policies and practices in this Notice cover the processing of Protected Personal Information (PPI) for clients of ABC Homeless Organization. All personal information that we maintain is covered by the policies and practices described in this privacy notice.
3. Protected Personal information (PPI) is any information we maintain about a client that:
   a. allows identification of an individual directly or indirectly.
   b. can be manipulated by a reasonably foreseeable method to identify a specific individual; or
   c. can be linked with other available information to identify a specific client. When this Notice refers to personal information, it means PPI.
4. We adopted this Policy because of standards for Homeless Management Information Systems (HMIS) issued by the United States Department of Housing and Urban Development (HUD). We intend our policies and practices to be consistent with those standards. See Homeless Management Information System (HMIS) Data Standards Revised Notice (March 2010).
5. This Notice tells our clients, our staff, and others how we process personal information. We follow the policies and practices described in this Notice.
6. We may amend this Notice and change our Policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment
7. A written copy of this Notice is available upon request.
8. A copy of this Notice is available on our website at www.abchomelessorganization.www.

B. How and Why We Collect Personal Information

1. We collect personal information only when appropriate to provide services, for another specific purpose of our organization, or when required by law. We may collect information for the following purposes:
   a. to provide or coordinate services to clients.
   b. to locate other programs that may be able to assist clients.
   c. for functions related to payment or reimbursement from others for services we provide.
   d. to operate our organization, including administrative functions such as legal, audits, personnel, oversight, and management functions.
   e. to comply with government reporting obligations; and
   f. when required by law.
2. We only use lawful and fair means to collect personal information.
3. We normally collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this Notice.
4. We may also get information about you from:
   a. individuals who are with you or are acting on your behalf
   b. other private organizations that provide services to you (i.e. non-profit organizations, faith-based organizations, for-profit organizations)
   c. government agencies (i.e. Department of Social Services, Social Security Administration)
   d. telephone directories and other published sources, including electronic sources.
5. We post a sign at our intake desk or other location explaining the reasons we ask for personal information.

C. How We Use and Disclose Personal Information

We collect personal information directly from you for reasons that are discussed in our Privacy Policy. We may be required to collect some personal information by law or by organizations that give us funding to operate our programs. Other personal information that we collect is important to run our programs, to improve services for homeless individuals and families, and to better understand the needs of homeless individuals and families. We only collect information that we consider to be appropriate and necessary for these purposes.

1. We use or disclose personal information for activities described in this part of the Notice. We may or may not make any of these uses or disclosures with your information. We assume that you consent to the use or disclosure of your personal information for the purposes described here and for other uses and disclosures that we determine to be compatible with these uses or disclosures:

   a. to **provide or coordinate services** to clients;

   b. for functions related to **payment or reimbursement for services**;

   c. to **carry out administrative functions** such as legal, audits, personnel, oversight, and management functions;

   d. to **create de-identified (anonymous) information** that can be used for research and statistical purposes without identifying clients;

   e. **when required by law** to the extent that use or disclosure complies with and is limited to the requirements of the law;

   f. to **avert a serious threat to health or safety** if

      (1) we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, **and**

      (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat;

   g. to **report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority** (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence

      (1) under any of these circumstances:

         (a) where the disclosure **is required** by law and the disclosure complies with and is limited to the requirements of the law;

         (b) if the individual agrees to the disclosure, **or**

         (c) to the extent that the disclosure is **expressly authorized** by statute or regulation, **and**

            (i) we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, **or**

            (ii) 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.

      and

(2) when we make a permitted disclosure about a victim of abuse, neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:

(a) we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, **or**

(b) we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment;

h. for **academic research purposes**

(1) conducted by an individual or institution that has a formal relationship with ABC Homeless Organization if the research is conducted either:

(a) by an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a designated program administrator (other than the individual conducting the research), **or**

(b) by an institution for use in a research project conducted under a written research agreement approved in writing by a designated program administrator.

and

(2) any written research agreement:

(a) must establish rules and limitations for the processing and security of PPI in the course of the research;

(b) must provide for the return or proper disposal of all PPI at the conclusion of the research;

(c) must restrict additional use or disclosure of PPI, except where required by law;

(d) must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, **and**

(e) is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

i. to a law enforcement official **for a law enforcement purpose** (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

(1) in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena

(2) if the law enforcement official makes a **written request** for PPI that:

(a) is signed by a supervisory official of the law enforcement agency seeking the PPI;

(b) states that the information is relevant and material to a legitimate law enforcement investigation;

(c) identifies the PPI sought;

(d) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, **and**

(e) states that de-identified information could not be used to accomplish the purpose of the disclosure;

(3) if we believe in good faith that the PPI constitutes **evidence of criminal conduct** that occurred on our premises

(4) 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**

(5) if

(a) 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**

(b) 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.

and

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

2. Before we make any use or disclosure of your personal information that is not described here, we seek your consent first.

D. <u>How to Inspect and Correct Personal Information</u>

1. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. To inspect, get a copy of, or ask for correction of your information, contact us by telephone, mail or electronic mail during normal business hours at our main office.

4. We may deny your request for inspection or copying of personal information if:
    a. the information was compiled in reasonable anticipation of litigation or comparable proceedings
    b. the information is about another individual (other than a health care provider or homeless provider)
    c. the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, **or**
    d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial
6. We may reject repeated or harassing requests for access or correction.

E. <u>Data Quality</u>

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

F. <u>Complaints and Accountability</u>

1. We accept and consider questions or complaints about our privacy and security policies and practices through any medium. An e-mail may be sent to info@ABChomelessorganization.www, or write to us at:

    ABC Homeless Organization
    123 Main Street
    Anytown, USA, 99999

2. We make every effort to respond to questions or complaints about our privacy and security policies and practices as expeditiously as possible. Responses are made via the same medium in which they are received.
3. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy Notice. Each staff member must receive and acknowledge receipt of a copy of this privacy Notice.