

---

# HAMPDEN COUNTY CONTINUUM OF CARE

---

## HMIS POLICIES AND PROCEDURES MANUAL

---

City of Springfield Office of Housing  
DRAFT October 2013

---

# Contents

SECTION 1: HMIS OVERVIEW .....	4
Definition of Homeless Management Information System (HMIS).....	4
HUD HMIS Requirement.....	4
Hampden County HMIS: HMIS Lead and System .....	4
Contributing HMIS Organizations (CHOs).....	5
Governance.....	5
Definitions of Key Terms.....	5
Policy Review and Amendment.....	7
SECTION 2: PARTICIPATION IN HMIS .....	8
Contribution of Data.....	8
Participation Agreement .....	8
CHO HMIS Administrator.....	8
Agency Profiles in HMIS.....	8
Authorization of HMIS Users; Access to HMIS .....	9
Training.....	9
User Agreements.....	9
Removing Authorized Personnel .....	9
SECTION 3: DATA COLLECTION AND SHARING .....	10
Collection of Data on Participants and Non-Participants .....	10
HMIS Data Collection Standards.....	10
Sharing Client Data .....	10
SECTION 4: PRIVACY PLAN .....	11
Data Collection Limitations.....	11
Purpose and Use Limitations .....	12
Openness: Privacy Notice .....	14

Access and Correction .....	14
Accountability .....	15
Protections for victims of domestic violence, dating violence, sexual assault, and stalking .....	15
SECTION 5: SECURITY PLAN .....	16
Security Officers.....	16
Annual Security Certification .....	16
Security awareness training and follow-up .....	16
Reporting security incidents .....	17
Disaster Recovery .....	17
Contracts and other arrangements .....	18
System Security .....	18
Hard Copy Security .....	19
Database Integrity .....	19
SECTION 6: DATA QUALITY PLAN .....	20
Data Quality Benchmarks and Controls.....	20
Roles and Responsibilities .....	22
Remedial Actions .....	23
SECTION 7: SANCTIONS.....	24
APPENDICES	
Appendix 1: Participation Agreement	
Appendix 2: HMIS User Account Request/Termination Form	
Appendix 3: User Agreement Form	
Appendix 4: Authorized User List Form	
Appendix 5: Data Collection Forms	
Appendix 6: CoC Agency HMIS Sharing Partnership Agreement	
Appendix 7: Client Consent for Data Sharing	
Appendix 8: Sample Data Collection Notice	
Appendix 9: Sample Privacy Notice	
Appendix 10: CHO Security Certification	

## SECTION 1: HMIS OVERVIEW

### Definition of Homeless Management Information System (HMIS)

A Homeless Management Information System (HMIS) is a locally administered electronic data collection tool used to record and store client-level information about the numbers, characteristics, and needs of persons who use homeless housing and supportive services or homelessness prevention services.

HMIS is essential to efforts to coordinate client services and inform community planning and public policy. Through HMIS, homeless individuals benefit from improved coordination within and among agencies, informed advocacy efforts, and policies that result in targeted services. Analysis of information gathered through HMIS is critical to the preparation of a periodic accounting of homelessness in Hampden County, including required HUD reporting.

### HUD HMIS Requirement

Since 2004, HUD has required recipients of Continuum of Care (CoC) Program funds to collect electronic data on their homeless clients in HMIS. HUD published HMIS Data and Technical Standards in the Federal Register in 2004. The HMIS Technical Standards were amended by HUD in 2010. In 2011, HUD published a proposed rule establishing HMIS requirements (76 FR 76917). The proposed rule requires that every CoC have an HMIS that is operated in compliance with the requirements of 24 CFR part 580.

### Hampden County HMIS: HMIS Lead and System

The Hampden County CoC has designated the City of Springfield as the CoC's HMIS Lead HMIS entity. The City employs the Hampden County HMIS Administrator/Security Officer to both assure the quality of data entered in the database and to support general usage by all programs using the system. This individual is also responsible for structural changes to the database to capture information, for developing necessary reports, and for overseeing privacy and security policies. The HMIS Administrator/Security Officer reports to the Director of the Office of Housing for the City of Springfield who is responsible for approving all policy decisions made by the HMIS Lead.

The CoC has selected Social Solutions' Efforts to Outcomes (ETO) to serve as the CoC's HMIS. Each Contributing HMIS Organization (CHO) has its own site on the software. ETO serves as a web-based direct data entry portal for organizations that use ETO as their data management system. ETO also serves as a Data Warehouse for the Hampden County CoC, enabling participating agencies to upload data to the Data Warehouse from project-level client management systems, so long as those systems meet all applicable HUD and CoC HMIS requirements as outlined in these policies and procedures. ETO is able to sync data with the Commonwealth's HMIS ASIST program, enabling real-time data-syncing between the Hampden County HMIS and the Massachusetts ASIST HMIS.

ETO meets all Health Insurance Portability and Accountability Act (HIPAA) standards for security, privacy and confidentiality.

## Contributing HMIS Organizations (CHOs)

All Hampden County recipients of grants from programs authorized by Title IV of the McKinney-Vento Act are required to contribute data to the CoC's HMIS, with the exception of victim service providers and providers of legal services.<sup>1</sup> In addition, all other Hampden County agencies that provide shelter, housing and services to homeless and at risk populations are encouraged to use the Hampden County HMIS database.

An agency that participates in HMIS, referred to as a CHO, must execute a Participation Agreement with the HMIS Lead and must agree to abide by the policies and procedures outlined in this document. CHOs oversee and are responsible for their client level data, are responsible for the integrity and security of their agency's client level data, and assume the liability for any misuse of the software by agency staff. Participating agencies are responsible for ensuring that their agency users comply with the policies and procedures outlined in this manual.

## Governance

The Hampden County CoC adopted an HMIS Governance Agreement in September 2013, which defines the roles and responsibilities of the CoC, the HMIS Lead, CHOs, and the CoC HMIS and Data Committee. These HMIS Policies and Procedures incorporate the terms of the HMIS Governance Agreement.

## Definitions of Key Terms

The section below defines key terms used throughout this document and HUD guidance regarding HMIS.

Comparable Database	A database that is not the CoC's official HMIS, but an alternative system that victim service providers and legal services providers may use to collect client-level data over time and to generate unduplicated aggregate reports based on the data, and that complies with the requirements of this part. Information entered into a comparable database must not be entered directly into or provided to an HMIS.
Continuum of Care (CoC)	The group composed of representatives from organizations including nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve veterans, and homeless and formerly homeless persons organized to carry out the responsibilities of a Continuum of Care established under 24 CFR part 578.

---

<sup>1</sup> Victim services providers are prohibited from entering client data into HMIS and must enter required data into a comparable database instead. Legal services providers are not prohibited from entering client-level data into HMIS, but may elect to use a comparable database instead of the HMIS, if the data is protected by attorney-client privilege.

Contributory HMIS Organization (CHO)	An organization that operates a project that contributes data to an HMIS.
Data Recipient	A person who obtains personally identifying information from an HMIS Lead or from a CHO for research or other purposes not directly related to the operation of the HMIS, Continuum of Care, HMIS Lead, or CHO.
Homeless Management Information System (HMIS)	The information system designated by Continuums of Care to comply with the requirements of 24 CFR part 580 and used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness.
HMIS Lead	The entity designated by the Continuum of Care in accordance with 24 CFR part 580 to operate the Continuum's HMIS on its behalf. The HMIS Lead for the Hampden County CoC is the City of Springfield.
HMIS Vendor	A contractor who provides materials or services for the operation of an HMIS. An HMIS vendor includes an HMIS software provider, web server host, data warehouse provider, as well as a provider of other information technology or support.
Protected Identifying Information (PII)	Information about a program participant that can be used to distinguish or trace a program participant's identity, either alone or when combined with other personal or identifying information, using methods reasonably likely to be used, which is linkable to the program participant.
Unduplicated Accounting of Homelessness	An unduplicated accounting of homelessness includes measuring the extent and nature of homelessness (including an unduplicated count of homeless persons), utilization of homelessness programs over time, and the effectiveness of homelessness programs.
User	An individual who uses or enters data in an HMIS or another administrative database from which data is periodically provided to an HMIS.
Victim Service Provider	A private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. This term includes rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs.

## Policy Review and Amendment

The Hampden County HMIS policies and procedures must comply with HUD regulations and/or technological changes. The HMIS Lead will review the policies and procedures annually and at the time of any change to the system management process, the data warehouse software, the methods of data exchange, or any HMIS data or technical requirements issued by HUD.

In the event that changes are required to the HMIS policies and procedures, the HMIS Lead will develop recommendations to the HMIS and Data Committee for review, modification, and approval. The HMIS and Data Committee will present the Board of Directors with recommended changes to the policies and procedures, and the new policies and procedures will be reviewed, modified, and voted on by the Board of Directors. The HMIS Lead will modify practices, documentation, and training material to be consistent with the revised policies and procedures within six months of approval.

## SECTION 2: PARTICIPATION IN HMIS

### Contribution of Data

Data may be contributed to HMIS in one of three ways:

1. Contribute directly to the Hampden County HMIS. Agencies that contribute directly are provided web-based log-in information with which to access the system.
2. Contribute data to the Commonwealth of Massachusetts ASIST program and sign a data-syncing agreement enabling the Hampden County HMIS and ASIST to share data.
3. Contribute data to a client management information system operated by a CHO that allows the CHO to collect the minimum required data elements and to meet other established minimum participation thresholds established by HUD, and regularly upload data from the CHO's system to the Hampden County HMIS.

All three types of contributors are subject to all relevant Hampden County HMIS policies and procedures.

### Participation Agreement

All CHOs that participate in the Hampden County HMIS must sign and agree to abide by the terms of the Participation Agreement, the contract between the CHO and the HMIS Lead. The Participation Agreement is attached to the policies and procedures as Appendix 1.

### CHO HMIS Administrator

Each CHO must designate an agency representative to act as the CHO's HMIS Administrator. CHO HMIS Administrators are responsible for the following:

- Communicate personnel/security changes for HMIS users to the Hampden County HMIS Administrator;
- Act as the first tier of support for agency HMIS users;
- Act as the liaison or contact between the agency and Hampden County HMIS Administrator;
- Ensure that the agency adheres to client privacy, confidentiality, and security policies;
- Maintain compliance with technical requirements for participation;
- Store and enforce end user agreements;
- Ensure that the Privacy Notice is being used;
- Enforce data collection, entry, and quality standards; and
- Attend monthly HMIS/Data Committee meetings.

### Agency Profiles in HMIS

Each agency must be set up in HMIS, with profiles that define the programs and services the agency offers, prior to HMIS use and data entry. Agencies should contact the Hampden County HMIS Administrator for agency set up. Agency Profiles will be reviewed and updated on an annual basis.



## Authorization of HMIS Users; Access to HMIS

Only authorized individuals who certify that they have completed the necessary on-line training and have signed and submitted the HMIS User Agreement will be provided a User name and password and allowed to access HMIS on behalf of their agency. The on-line training is available at \_\_\_\_\_.

To add a new agency HMIS User, a CHO must submit a completed copy of the HMIS User Account Request/Termination Form to the Hampden County HMIS Administrator. The HMIS User Account Request/Termination Form is attached to this Manual as Appendix 2. Each CHO Site Administrator should keep an updated list of approved agency users; this document should be submitted to the Hampden County HMIS Administrator on a quarterly basis. The Authorized User List form is attached to this manual as Appendix 3.

The HMIS Administrator will provide each new HMIS User with a unique user name and password. The HMIS User must change the password the first time he/she logs into the system.

## Training

The City of Springfield uses an on-line training module to provide initial training to new HMIS users regarding privacy and security measures, and all users are required to complete the training module before being issued a password.

The City of Springfield offers regular training in system use for CHO HMIS Administrators and expects these sessions to operate in a “train-the-trainer” model, in which CHO HMIS Administrators will be responsible for training their agency’s HMIS users to use the system for data input. Each CHO HMIS Administrator must attend Hampden County HMIS Administrator training.

## User Agreements

A Hampden County HMIS User Agreement (Appendix 3) must be signed and kept for all agency personnel or volunteers that will collect or use HMIS data on behalf of the agency. Agencies must store signed Hampden County HMIS User Agreements for 7 years for each individual that will collect/enter HMIS data. Agencies should never dispose of a signed Hampden County HMIS End User Agreement upon revoking an individual's authorization or in terminating an individual's employment.

## Removing Authorized Personnel

The Hampden County HMIS Administrator must be notified within one business day when an individual is no longer authorized to access HMIS on the agency’s behalf. CHOs must send a completed HMIS User Account Request/Termination Form (Appendix 2) to the Hampden County HMIS Administrator via email to [dmerkman@springfieldcityhall.com](mailto:dmerkman@springfieldcityhall.com) or fax to 413-787-6515. When a CHO provides an HMIS User Account Request/Termination Form to the Hampden County HMIS Administrator, it must also provide an updated Authorized User List (Appendix 4). Upon receipt of the request, the Hampden County HMIS System Administrator will immediately deactivate the individuals' HMIS user account.

## SECTION 3: DATA COLLECTION AND SHARING

### Collection of Data on Participants and Non-Participants

Agencies should collect data from families and individuals who are homeless or at risk of becoming homeless and are accessing services from their agency. Agencies may also choose to collect data for HMIS on individuals or families that make contact with the agency, but are not able to receive services from the agency. Information must be collected separately for each family member, and all family member data must be entered into the database.

### HMIS Data Collection Standards

Agencies may choose to enter data directly into the HMIS or to collect client level data on paper prior to entering into HMIS. If agencies use paper data collection forms, all hard copy forms and services must be entered into the database within 48 hours or within 24 hours for emergency shelter providers. Whether direct data entry or paper forms are used the data collected and entered must be consistent with the data provided by the client and the hard copy data collection form the CoC provides.

There are four HMIS forms used by the CoC for data collection: the Universal, Program-Specific, Interim Assessment and Exit forms. These forms are included in this Manual at Appendix 5. If information is being collected on a family, information must be collected on each member of the family.

All programs must use the Universal form. Agencies receiving funds from federal homeless assistance grants are required to use the Program-Specific forms, Interim Assessment Form and Exit form. Agencies not receiving these types of funds may choose to use the Universal forms.

Agencies that are not required to complete the Program-Specific data fields are strongly recommended to collect these pieces of information, depending upon the type of programs and services the agency offers. The additional data points on the client will prove extremely helpful for the agency when reporting on client outcome measurement/progress, internal accounting for service delivered, and external reporting to funders.

### Sharing Client Data

HMIS allows groups of agencies to share the same client record, as a means of improving client services and successful referrals. Clients will have the ability to decide if they want their information shared, unless the program/agency entering requires data sharing.

HMIS client data may be shared only in accordance with the Interagency Data Network Sharing Agreement, attached as Appendix 7. Prior to sharing data with another agency, the CHO must obtain a signed Client Consent for Data Sharing. The client consent form is attached as Appendix 8.

## SECTION 4: PRIVACY PLAN

All CHO's must comply with the baseline privacy requirements described in these policies and procedures. A CHO must comply with federal, state and local laws that require additional confidentiality protections. When a privacy or security standard conflicts with other Federal, state, and local laws to which the CHO must adhere, the CHO must contact the HMIS Lead and collaboratively update the applicable policies for the CHO to accurately reflect the additional protections.

All privacy protections must be described in the CHO's Privacy Notice. A CHO must comply with all privacy protections included in its Privacy Notice.

### Data Collection Limitations

A CHO may collect Protected Identifying Information (PII) only when appropriate to the purposes for which the information is obtained or when required by law.

A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge or consent of the individual. A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. Consent of the individual for data collection may be inferred from the circumstances of the collection.

Providers may use the following language to meet this standard:

We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.

Agencies must also post the data collection notice in any language other than English that is spoken by a significant percentage of their clients (5% or more); for most agencies in Hampden County, this will require that the sign be posted in Spanish. The Spanish translation of the statement follows:

Recopilamos información personal directamente de usted por las razones que se discuten en nuestra declaración de privacidad. Podemos ser requeridos recopilar alguna información personal por ley o por las organizaciones que nos dan dinero para operar este programa. Otra información personal que recopilamos es importante para ejecutar nuestros programas, mejorar los servicios para las personas sin hogar, y para comprender mejor las necesidades de las personas sin hogar. Nosotros solamente recopilamos información que consideramos apropiado.

The data collection notice is provided in English and Spanish in Appendix 8. CHO's may photocopy these notices directly or may create their own notices that inform clients about data collection.

## Purpose and Use Limitations

A CHO must specify in its Privacy Notice the purposes for which it collects PII and must describe all uses and disclosures. A CHO may infer consent for all uses and disclosures specified in HUD HMIS Technical Notices and regulations notice and for uses and disclosures determined by the CHO to be compatible with those specified by HUD. Uses and disclosures not specified in the Privacy Notice can be made only with the consent of the individual or when required by law.

### Allowable HMIS Uses and Disclosures of PII

A CHO may use or disclose PII from an HMIS under the following circumstances: (1) To provide or coordinate services to an individual; (2) for functions related to payment or reimbursement for services; (3) to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or (4) for creating de-identified PII.

CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of clients. The following additional uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible and limited way.

#### *1. Uses and disclosures required by law*

A CHO may use or disclose PII when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

#### *2. Uses and disclosures to avert a serious threat to health or safety*

A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if: (1) the CHO, in good faith, believes 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.

#### *3. Uses and disclosures about victims of abuse, neglect or domestic violence*

CHO may disclose PII about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following circumstances:

- Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
- If the individual agrees to the disclosure; or
- To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a

law enforcement or other public official authorized to receive the report represents that the PII 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.

A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

- The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- The CHO would be informing a personal representative (such as a family member or friend), and the CHO 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 CHO, in the exercise of professional judgment.

#### *4. Uses and disclosures for academic research purposes*

A CHO may use or disclose PII for academic research conducted by an individual or institution that has a formal relationship with the CHO if the research is conducted either:

- By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the CHO; or
- By an institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the CHO.

#### *5. Disclosures for law enforcement purposes*

A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII for a law enforcement purpose to a law enforcement official under any of the following circumstances:

- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
- If the law enforcement official makes a written request for protected personal information that: (1) Is signed by a supervisory official of the law enforcement agency seeking the PII; (2) states that the information is relevant and material to a legitimate law enforcement investigation; (3) identifies the PII sought; (4) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (5) states that de-identified information could not be used to accomplish the purpose of the disclosure.

- If the CHO believes in good faith that the PII constitutes evidence of criminal conduct that occurred on the premises of the CHO;
- In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PII 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 PII 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.

## Openness: Privacy Notice

A CHO must publish a Privacy Notice describing its policies and practices for the processing of PII and must provide a copy of its Privacy Notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its Privacy Notice on the web page. A CHO must post a sign stating the availability of its Privacy Notice to any individual who requests a copy.

If any language other than English is spoken by a significant percentage of an agency's clients (5% or more), the privacy notice must be provided in that language. A sample Privacy Notice in English and Spanish is attached to this document as Appendix 9; it may be adopted as is or amended by a CHO.

A CHO must state in its Privacy Notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. An amendment to the Privacy Notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. A CHO must maintain permanent documentation of all Privacy Notice amendments.

## Access and Correction

In general, a CHO must allow an individual to inspect and to have a copy of any PII about the individual. A CHO must offer to explain any information that the individual may not understand. A CHO must consider any request by an individual for correction of inaccurate or incomplete PII pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

In its privacy notice, a CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PII:

1. Information compiled in reasonable anticipation of litigation or comparable proceedings;
2. Information about another individual (other than a health care or homeless provider);

3. 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; or
4. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A CHO can reject repeated or harassing requests for access or correction. A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

## **Accountability**

A CHO must require staff to sign an agreement that acknowledges receipt of a copy of the Privacy Notice and that pledges to comply with the Privacy Notice. The Hampden County HMIS User agreement contains this language and enables each CHO to meet this requirement.

A CHO must establish a written policy for accepting and considering questions or complaints about its privacy and security policies and practices.

## **Protections for victims of domestic violence, dating violence, sexual assault, and stalking**

The Violence against Women Act and Department of Justice Reauthorization Act of 2005 (42 U.S.C. 13925) prohibits victim service providers from entering data into HMIS. Victim service providers that are recipients of funds requiring participation in HMIS, but which are prohibited from entering data into an HMIS, must use a comparable database. A comparable database means a database used by a victim service provider that collects client-level data over time and generates unduplicated aggregate reports based on the data, in accordance with HUD requirements. Information entered into a comparable database must not be entered directly into or provided to an HMIS.



## SECTION 5: SECURITY PLAN

Security standards ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users. Security standards must be followed by the HMIS Lead and CHOs.

### Security Officers

The HMIS Lead must designate a Hampden County HMIS Security Officer. The duties of the HMIS Lead Security Officer include, but may not be limited to:

- Review the Security Plan annually and at the time of any change to the security management process, the data warehouse software, the methods of data exchange, and any HMIS data or technical requirements issued by HUD. In the event that changes are required to the HMIS Security Plan, work with the HMIS and Data Committee for review, modification, and approval.
- Confirm that the HMIS Lead adheres to the Security Plan or develop and implement a plan for mitigating any shortfall.
- Respond to any security questions, requests, or security breaches to the Hampden County HMIS System and communicate security-related HMIS information to CHOs.

Each CHO must designate a CHO HMIS Security Officer. The duties of the CHO Security Officer include, but may not be limited to:

- Confirm that the CHO adheres to the Security Plan or provide and implement a plan for mitigating any shortfall, including milestones to demonstrate elimination of the shortfall over time.
- Communicate any security questions, requests, or security breaches to the Hampden County CoC HMIS System Administrator/Security Officer, and security-related HMIS information relayed from the Hampden County HMIS System Administrator to the CHO's end users.
- Complete security training offered by the HMIS Lead.

### Annual Security Certification

The HMIS Lead and each CHO must complete an annual security review to ensure the implementation of the security requirements for the HMIS. This security review must include completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan. Each CHO Security Officer must complete the Security Self-Certification each January using the form provided in Appendix 12, and submit the completed form to the CoC Administrator/Security Officer no later than February 1 of each year.

### Security awareness training and follow-up

All users must receive security training prior to being given access to the HMIS. The HMIS Lead has created an on-line security and privacy training module which must be completed prior to being issued a



password. The request for new password requires a certification that the new user has completed the on-line training. In addition, the HMIS Lead shall provide security training no less than once per year.

## **Reporting security incidents**

The HMIS Lead has created the following policy and chain of communication for reporting and responding to security incidents.

### ***Security Incidents***

All HMIS users are obligated to report suspected instances of noncompliance with these policies and procedures that may leave HMIS data vulnerable to intrusion. Each CHO is responsible for reporting any security incidents involving the real or potential intrusion of the Hampden County HMIS to the HMIS Lead. The HMIS Lead is responsible for reporting any security incidents involving the real or potential intrusion of the Hampden County HMIS to the Hampden County CoC Steering Committee.

### ***Reporting Threshold***

HMIS users must report any incident in which unauthorized use or disclosure of PII has occurred. CHO users will report any incident in which PII may have been used in a manner inconsistent with the CHO Privacy or Security Policies. Security breaches that have the possibility to impact the Hampden County HMIS must be reported to the HMIS Administrator.

### ***Reporting Process***

HMIS users will report security violations to their CHO HMIS Administrator/CHO Security Officer. The CHO HMIS Administrator will report violations to the HMIS Lead Security Officer. Any security breaches identified by Social Solutions ETO will be communicated to the HMIS Lead Security Officer and System Administrator. The HMIS Lead Security Officer, in cooperation with the System Administrator, will review violations and recommend corrective and disciplinary actions to the HMIS and Data Committee and the Steering Committee, as appropriate. Each CHO will maintain and follow procedures related to internal reporting of security incidents.

### ***Audit Controls***

Social Solutions maintains an accessible audit trail within ETO that allows the System Administrator to monitor user activity and examine data access for specified users. Activity will be monitored by Social Solutions and potential or actual security incidents will be reported to the HMIS Lead. Additionally, the System Administrator will monitor audit reports for any apparent security breaches or behavior inconsistent with the Privacy Policy outlined in these policies and procedures.

## **Disaster Recovery**

Hampden County HMIS data is stored by Social Solutions in secure and protected off-site locations with duplicate back-up. In the event of disaster, the HMIS Administrator will coordinate with Social Solutions to ensure the HMIS is functional and that data is restored. Each CHO must have a plan for recovering access to its own data.

## **Contracts and other arrangements**

The HMIS Lead shall retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or required to comply with HUD requirements for a seven year period.

## **System Security**

Each CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes and servers.

### ***User Authentication***

A CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

### ***Virus Protection***

A CHO must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

### ***Firewalls***

A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall as long as the server has a firewall.

### ***Physical Access to Systems with Access to HMIS Data***

A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff is not present, steps should be taken to ensure that computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.

## Hard Copy Security

A CHO must secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PII when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.

Hard copies of data stored or intended to be stored in HMIS, regardless of whether the data has yet been entered into HMIS, will be treated in the following manner:

1. Records shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, records shall be maintained in such a manner as to prevent exposure of PII to anyone other than the user directly utilizing the record.
3. Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the CHO's place of business and where return of the records by the close of business would result in the undue burden on staff.
4. When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not re-disclose the PII contained in those records except as permitted by these policies and procedures.
5. Faxes or other printed documents containing PII shall not be left unattended.
6. Fax machines and printers shall be kept in secure areas.
7. When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
8. When finished faxing, copying or printing all documents containing PII should be removed from the machines promptly.

## Database Integrity

The CHO must not intentionally cause corruption of the Hampden County HMIS in any manner. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, will result in immediate suspension of HMIS licenses held by the CHO, and suspension of continued access to the Hampden County MIS by the CHO.

The City will investigate all potential violations of any security protocols. Any user found to be in violation of security protocols will be subject to sanctions, as described in Section 7 of this Manual. An individual users may be subject to disciplinary action by the employer CHO.

## SECTION 6: DATA QUALITY PLAN

Data quality standards ensure the completeness, accuracy, and consistency of the data in the HMIS. The Continuum of Care is responsible for the quality of the data produced.

Data Quality is critical for the CoC to: measure the nature and extent of homelessness; meet the CoC's local homeless data and planning needs; and complete required HUD reporting, including Annual Performance Reports (APRs), the Annual Homeless Assessment Report (AHAR), the Point-in-Time (PIT) Count, and the Housing Inventory Count (HIC).

### Data Quality Benchmarks and Controls

The chart below identifies the specific standards that the CoC will monitor as part of its data quality plan, as well as the monitoring procedures for each standard. The Coverage principle applies to the CoC as a whole. All other standards apply to CHOs and programs.

General Principle	Specific Principle	Expected Benchmark	Monitoring Procedure Who? How often?
Coverage	All lodging and non-lodging homeless programs in the CoC report HMIS data	100% Emergency shelter beds, Safe Havens, Outreach, Rapid Rehousing and SSVF report HMIS.  86% Transitional housing and permanent supportive housing beds report HMIS.	HIC provides annual report.  HMIS Lead will report status quarterly to Board of Directors.
Completeness	All clients entered	95% of clients must have all universal data entered.  95% of clients must have an assessment.  95% of clients qualifying for mid-term assessment must have assessment completed.	Monthly reports sent to participating agencies.

	Complete exit data entered	No more than 5 missing exit assessments.  No more than 5 incomplete exits assessments (includes completion of exit assessment)	Check missing exit assessments on monthly missing data report.  The HMIS Administrator will spot check 6 sites every month, checking recent exit assessments for completeness.
	All services entered	All clients must have at least one service record.	For McKinney run Q 15 of APR monthly and check against number of active clients.
Accuracy	Truthfulness from clients	5 of the 6 records must be complete.	Annual visit to conduct random spot check of paper files against HMIS. Pull 6 records and look for client data in the database.
	Accurate data entered by staff	The APR and other annual or quarterly reports must match the data in the database.	The HMIS Administrator will check all submitted reports against data in the database. No report will be accepted if there is a discrepancy between the two sources.
	Changing data kept up to date	Active clients should be reviewed by the local database administrator every 30 days.	The Springfield HMIS Administrator will review with the local HMIS Administrator in quarterly visits.
Timeliness	Data are entered soon after collected	Clients must be entered within 48 hours of intake.  Emergency shelter clients must be entered within 24 hours of intake.	Monthly reports to agencies.

Consistency	Common interpretation of questions and answers	Data will be reviewed at the monthly data management meetings.	<p>The HMIS Administrator will compare aggregate data by users for same population to look for unusual patterns on a quarterly basis.</p> <p>Inconsistencies found during the month will be noted and discussed at the monthly data management meetings.</p>
	Common knowledge of what fields to answer	95% of required fields completed	Monthly check of required fields in system – 95% of records have complete minimal fields.

## Roles and Responsibilities

### CoC Board of Directors

The Board of Directors is responsible for oversight of data quality, and will review high-level data quality reports quarterly. The Board will act upon recommendations made by the HMS and Data Committee and the HMIS Lead.

### HMIS and Data Committee

The HMIS and Data Committee is responsible for ongoing oversight of progress toward the CoC's meeting of all Data Quality Benchmarks system-wide. It will regularly review data quality reports, assist agencies in gaining compliance, and ensure that required reports and trainings are made available for the agencies. It will provide quarterly updates to the CoC Board of Directors on progress of the data quality plan and provide regular reports on the quality of the CoC's data.

### HMIS Lead- City of Springfield

The HMIS Lead is responsible for monitoring CHOs to ensure that the standards on the extent and quality of data entered into the Hampden County HMIS set forth in these policies and procedures are met to the greatest possible extent and that data quality issues are quickly identified and resolved.

The HMIS Lead will run data quality reports on a quarterly basis and will directly provide agencies with the reports for their projects via email.

Monthly data quality reports are run on the 9<sup>th</sup> of each month and are sent to each participating agency by the HMIS Administrator on the 15<sup>th</sup> of every month. The regularity of the reporting provides participating agencies with the opportunity to review data and update any missing elements before the

HMIS Administrator assesses progress. Monthly reports include the following.

1. **Progress reports on expected contractual outcomes.** Each funded project has specific target requirements. Specific reports are created for each project to show the agency's progress to date on their contractual agreements. Both the dates and methods of tracking information vary according to the particular project.
2. **Missing Data – Assessments:** This report alerts participating agencies if they have failed to record detailed assessment information. It identifies where they have entered a new participant into the database, but have failed to provide required assessments.
3. **Missing HUD Universal Data Elements:** The HMIS Administrator will track completion of universal data elements on a monthly basis.

The City of Springfield will monitor at least annually the projects that are funded by the CoC. It will review data quality reports, bed utilization reports, and compliancy with the Data Quality Plan. It will report and make recommendations to the CoC Application Committee on the quality and usability of data submitted by CoC-funded agencies.

### Contributing HMIS Organizations

CHOs are responsible for training and monitoring HMIS users to ensure understanding of and compliance with data quality standards.

Each CHO is responsible for addressing any issues identified through the data quality monitoring. Where data errors are identified, the CHO must correct the errors within 30 days. Where overall systemic data quality issues are identified, the CHO must participate with the HMIS Lead in creation of a corrective action plan

### Remedial Actions

The goal of data quality monitoring is for the CoC to obtain and maintain high-quality data. In order to meet this goal, CHOs with repeated data quality issues will be initially provided with increasing levels of support to assist in resolving data issues. Support may include additional training and/or technical assistance from the HMIS Lead, Social Solutions, or a qualified consultant.

The CHO may be required to submit a corrective action plan to the HMIS Lead, and to provide regular reports to the HMIS Lead on progress toward implementing the identified corrective actions. Components of a corrective action plan may include:

- Developing and following a schedule of actions for carrying out HMIS-related tasks, including schedules, timetables, and milestones;
- Establishing and following an HMIS data quality plan that assigns responsibilities for carrying out remedial actions; and
- Increased monitoring and reporting of HMIS data quality.

If increased support does not result in the CHO meeting data quality standards, the CHO may be subject to sanctions, as described in Section 7 of this Manual.

## SECTION 7: SANCTIONS

Sanctions may be imposed for violations of privacy or confidentiality standards, or ongoing failure to meet data quality standards.

### Available Sanctions

Sanctions include the following:

- Suspending funds disbursement;
- Suspending or terminating access to HMIS;
- Reducing or terminating the remaining grant;
- Imposing conditions on future grants; and
- Imposing other legally available remedies.

CHOs subject to sanctions may not apply for new CoC Program or Emergency Solutions Grant Program funds. CHO's who have lost access to the Hampden County HMIS due to sanctions may not apply for CoC Program renewal funds.

### Sanctions Procedure

Sanctions may only be imposed by the CoC Board of Directors. An initial recommendation that sanctions be imposed is generated by the HMIS Lead, and is presented to the HMIS and Data Committee. The HMIS and Data Committee will make a recommendation to the Board of Directors regarding specific sanctions to be imposed. The Board may impose the recommended sanction, or a different sanction that it believes is appropriate.

### Sanctions Separate from Project Review for Renewal

Each CHO's record of compliance with the policies and procedures set forth in this Manual and the level of data quality achieved will be reported to the CoC Application Committee, which may take these factors into consideration in determining which projects will be submitted for renewal, and which agencies may be permitted to apply for new project funding.

Decisions of the CoC Application Committee are separate and distinct from decisions concerning imposition of sanctions.



## Appendix 1: Participation Agreement

DRAFT

## HAMPDEN COUNTY HMIS Participation Agreement

This agreement is entered into on \_\_\_\_\_(date) between the City of Springfield, hereafter known as "City", and \_\_\_\_\_ (agency name), hereafter known as the "Contributing HMIS Organization" or "CHO," regarding access and use of the Hampden County Continuum of Care Homeless Management Information System, hereafter known as "Hampden County HMIS."

### I. Introduction

The Hampden County HMIS, a shared human services database, allows authorized personnel at homeless and human service provider agencies throughout Hampden County to enter, track, and report on information concerning their own clients and to share information, subject to appropriate inter-agency agreements, on common clients.

The HMIS goals are to:

- Improve coordinated care for and services to homeless persons in Hampden County;
- Provide a user-friendly and high quality automated records system that expedites client intake procedures, improves referral accuracy, and supports the collection of quality information that can be used for program improvement and service-planning; and
- Meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD) and other funders as needed.

In compliance with all state and federal requirements regarding client/consumer confidentiality and data security, the Hampden County HMIS is designed to collect and deliver timely, credible, quality data about services and homeless persons or persons at risk for being homeless. The Hampden County Continuum of Care has selected Social Solutions Efforts to Outcomes (ETO) as its HMIS application, and the HMIS is administered by the City as the HMIS Lead.

### II. HMIS Lead Responsibilities

1. The City will provide the CHO 24-hour access to the HMIS data-gathering system, via internet connection.
2. The City will provide model Data Collection notices, Privacy Notices, Client Release forms and other templates for agreements that may be adopted or adapted in the CHO's implementation of HMIS functions.
3. The City will provide both initial training and periodic updates to that training for core CHO staff regarding the use of the HMIS, with the expectation that the CHO will take responsibility for conveying this information to all CHO staff using the system.

4. The City will provide basic user support and technical assistance (i.e., general trouble-shooting and assistance with standard report generation). Access to this basic technical assistance will normally be available from 8:15 AM to 4:30 PM on Monday through Friday (with the exclusion of holidays).
5. The City will not publish reports on data concerning or provided by applicants for and recipients of benefits and services that identify specific persons. Public reports, including but not limited to the HUD Annual Homeless Assessment Report (AHAR) as required by Congress, will be limited to presentation of aggregated data within the Hampden County HMIS database.
6. The publication practices of the City will be governed by policies established by relevant CoC committees and will include qualifiers such as coverage levels or other issues necessary to clarify the meaning of published findings.

### **III. CHO Responsibilities**

1. The CHO Executive Director or authorized signatory will designate a CHO HMIS Administrator who will assume responsibility for providing ongoing user support to all users within the CHO, including but not limited to the training of any staff person prior to issuance of a user account.
2. The CHO will enter all minimum required data elements as defined for all persons who are participating in services funded by the U.S. Department of Housing and Urban Development (HUD) Supportive Housing Program, Shelter + Care Program, Emergency Shelter Grant (ESG) Program or Housing Opportunities for Persons with AIDs (HOPWA). The CHO will enter data in a consistent manner, and will strive for real-time, or close to real-time, data entry.
3. The CHO will routinely review records it has entered in the HMIS for completeness and data accuracy. The review and data correction process will be made according to Hampden HMIS' published Policies and Procedures.
4. The CHO will not knowingly enter inaccurate information into HMIS.
5. The CHO will review and assess data entered into the Hampden County HMIS, and will enter data revisions as necessary, to reflect a change in the status of an applicant for or a recipient of benefits or services, enter updates, or edit incorrect information.
6. The CHO will utilize the HMIS for business purposes only.
7. The CHO will keep updated virus protection software on agency computers that access the HMIS.
8. Transmission of material in violation of any United States Federal or State regulations is prohibited.
9. The CHO will not use the HMIS with intent to defraud the Federal, State, or local government, or an individual entity, or to conduct any illegal activity.
10. The CHO agrees to designate at least one specific staff member to regularly attend HMIS and Data Committee meetings and other local or regional User Meetings to discuss procedures, updates, policy and practice guidelines, data analysis, and software/ hardware upgrades.
11. Notwithstanding any other provision of this Participation Agreement, the CHO agrees to abide by all policies and procedures relevant to the use of HMIS that the City or the Hampden County CoC publishes from time to time.

## **IV. Privacy and Confidentiality**

### **A. Protection of Client Privacy**

1. The CHO will comply with all applicable federal, state and local laws regarding protection of client privacy.
2. The CHO will comply specifically with Federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records.
3. The CHO will comply specifically with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R., Parts 160 & 164, and corresponding regulations established by the U.S. Department of Health and Human Services.
4. The CHO will comply with 201 CMR 17:00 Standards for the Protection of Personal Information of Residents of the Commonwealth, and will comply with Massachusetts Executive Order 504.
5. The CHO will comply with all policies and procedures established by the City of Springfield/Hampden County HMIS pertaining to protection of client privacy.

### **B. Client Confidentiality**

1. The CHO agrees to post a data collection sign that meets the requirements of the Hampden County HMIS Policies and Procedures at all intake locations. The CHO will also make available the Hampden HMIS Privacy Notice (or an acceptable agency-specific alternative) to each consumer, and post the Privacy Notice on the CHO's website. The CHO will provide a verbal explanation of the HMIS and arrange for a qualified interpreter/translator in the event that an individual is not literate in English or has difficulty understanding the Data Collection notice, the Privacy Notice or associated Consent Form.
2. The CHO will not solicit or enter information from clients into the HMIS database unless it is essential to provide services, report to CHO funders, or conduct evaluation or research.
3. The CHO will not divulge any confidential information received from the HMIS to any organization or individual without proper written consent by the client, unless otherwise permitted by applicable regulations or laws.
4. The CHO will ensure that all persons who are issued a User Identification and Password to the HMIS abide by this Participation Agreement, including all associated confidentiality provisions. The CHO will be responsible for oversight of its own related confidentiality requirements.
5. The CHO agrees that it will not request a User ID and Password for any person until the individual completes the CoC's online Privacy and Security training module.
6. The CHO acknowledges that ensuring the confidentiality, security and privacy of any information downloaded from the system by the CHO is strictly the responsibility of the CHO.
7. The CHO agrees that it will establish a procedure for accepting and considering questions or complaints about its privacy and security policies and procedures.

### ***C. Inter-Agency Sharing of Information***

1. The CHO acknowledges that all forms provided by Hampden County HMIS regarding client privacy and confidentiality are shared with the CHO as generally applicable models that may require specific modification in accord with CHO-specific rules. The CHO will review and revise (as necessary) all forms provided by HMIS to assure that they are in compliance with the laws, rules and regulations that govern its organization but in no case shall the agency relax any confidential rules established by this Participation Agreement or any other Hampden County HMIS policy or procedure.
2. The CHO agrees to develop a plan for all routine sharing practices with partnering CHOs and document that plan through a fully executed Interagency Data Network Sharing Agreement (IDNSA).
3. The CHO acknowledges that informed client consent is required before client information is shared with other CHOs in the system. The CHO will document client consent on the HMIS Client Consent - Release of Information for Data Sharing.
4. If the client has given approval through a completed HMIS Client Consent - Release of Information for Data Sharing, the Agency may share information according to IDNSA that the CHO has negotiated with other partnering agencies in HMIS.
5. The CHO will incorporate an HMIS release clause into its IDNSA(s) if the CHO intends to share restricted client data within the HMIS. Restricted information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns shall not be shared with other participating Agencies without the client's written, informed consent as documented on the CHO-modified Client Consent - Release of Information for Data Sharing. Sharing of restricted information must also be planned and documented through a fully executed IDNSA.
6. CHOs with whom information is shared are each responsible for obtaining appropriate consent(s) before allowing further sharing of client records.
7. The CHO acknowledges that the CHO, itself, bears primary responsibility for oversight for all sharing of data it has collected via the HMIS. The CHO agrees to place all Client Consent - Release of Information for Data Sharing forms related to the HMIS in a file to be located at the CHO's business address and that such forms will be made available to the City for periodic audits. The CHO will retain these HMIS-related Client Consent - Release of Information for Data Sharing forms for a period of seven (7) years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
8. The CHO acknowledges that clients who choose not to authorize sharing of information cannot be denied services for which they would otherwise be eligible.

### ***D. Custody of Data***

1. The CHO acknowledges, and the City agrees, that the CHO retains ownership over all information it enters into the HMIS.
2. In the event that the Hampden County HMIS ceases to exist, member CHOs will be notified and provided reasonable time to access and save client data on those served by the agency, as well

as statistical and frequency data from the entire system. Thereafter, the information collected by the centralized server will be purged or appropriately stored.

3. In the event that the Hampden County CoC ceases to exist, or the City ceases its service as the CoC's HMIS Lead, the custodianship of the data within HMIS will be transferred by the City to another organization for continuing administration, and all CHOs will be informed in a timely manner.

## **V. Publication of Reports**

1. The CHO agrees that it may only release aggregated information generated by the HMIS that is specific to its own services.
2. The CHO acknowledges that the release of aggregated information will be governed through policies established by relevant committees operating at the Continuum of Care level. Such information will include qualifiers such as coverage levels or other issues necessary to fully explain the published findings.

## **VI. Database Integrity and Sanctions**

1. The CHO will comply with the security standards set forth in the HUD HMIS standards and the Hampden County HMIS Policies and Procedures Manual, including establishment of mechanisms to protect hardcopy data. The CHO will not share assigned User ID's and Passwords to access the HMIS with any other organization, governmental entity, business, or individual.
2. The CHO will not intentionally cause corruption of the HMIS in any manner. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, will result in immediate suspension of services, and, where appropriate, legal action against the offending entities.
3. The City will investigate all potential violations of any security protocols. Any user or CHO found to be in violation of security protocols will be sanctioned. Sanctions may include, but are not limited to:
  - a. Suspending or terminating access to HMIS;
  - b. Suspending funds disbursement;
  - c. Reducing or terminating the remaining grant;
  - d. Imposing conditions on future grants; and
  - e. Imposing other legally available remedies.
4. The Agency's access may be suspended or revoked if serious or repeated violation(s) of HMIS Policies and Procedures occur by Agency users. Agencies that lose the ability to contribute HMIS may not receive CoC Program or ESG funding.

## **VII. Hold Harmless**

1. The City makes no warranties, expressed or implied. The CHO, at all times, will indemnify and hold the City harmless from any damages, liabilities, claims, and expenses that may be claimed against the CHO; or for injuries or damages to the CHO or another party arising from participation in the

HMIS; or arising from any acts, omissions, neglect, or fault of the CHO or its agents, employees, licensees, or clients; or arising from the CHO's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. The CHO will also hold the City harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Social Solutions, by the CHO's or other CHO's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. The City shall not be liable to the CHO for damages, losses, or injuries to the CHO or another party other than if such is the result of gross negligence or willful misconduct of the City.

2. The CHO agrees to keep in force a comprehensive general liability insurance policy with combined single limit coverage of not less than five hundred thousand dollars (\$500,000). Said insurance policy shall include coverage for theft or damage of the CHO's HMIS-related hardware and software, as well as coverage of CHO's indemnification obligations under this agreement.
3. Provisions of Section VII shall survive any termination of the Participation Agreement.

#### **VIII. Terms and Conditions**

1. The parties hereto agree that this Participation Agreement is the complete and exclusive statement of the agreement between parties and supersedes all prior proposals and understandings, oral and written, relating to the subject matter of this agreement.
2. The CHO shall not transfer or assign any rights or obligations under the Participation Agreement without the written consent of the City.
3. This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term is if allegations or actual incidences arise regarding possible or actual breeches of this agreement. Should such situations arise, the HMIS may immediately suspend access to the HMIS until the allegations are resolved in order to protect the integrity of the system.
4. This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.
5. The parties agree that Hampden County CoC is a third-party beneficiary of this contract and may enforce the terms and provisions of this contract as applicable. Further, the terms, conditions and agreements contained in this Participation Agreement may not be changed without the express written consent of the Hampden County CoC.
6. The Participation Agreement contains the entire agreement between the parties and supersedes all agreements, representations, warranties, statements, promises and understandings, whether oral or written, with respect to the subject matter hereof, and no party hereto shall be bound by or changed with any oral or written agreements, representations, warranties, statements, promises or understandings not specifically set forth in this Participation Agreement. Any change, modification, or waiver must be in writing and signed by both parties.
7. Neither party shall assign or transfer its rights, responsibilities or obligations under this Participation Agreement.

8. In the event that any provision of this Participation Agreement shall be held invalid or unenforceable, the same shall not affect in any respect whatsoever the validity or enforceability of the remainder of this Participation Agreement.
9. This Participation Agreement shall be executed in any number of counterparts, each of which, when executed and delivered, shall be an original, but all of which shall together constitute one in the same instrument.
10. This Participation Agreement shall be governed by, construed and enforced in accordance with the laws of the Commonwealth of Massachusetts. All parties hereby agree to the jurisdiction of the courts of the Commonwealth of Massachusetts with respect to any legal proceedings arising out of this Agreement, and further agree to Springfield, Massachusetts as the place of venue for any such action.

IN WITNESS WHEREOF, the parties have entered into this Participation Agreement:

**CHO:** \_\_\_\_\_

Address: \_\_\_\_\_

Name & Title of Authorized Signature: \_\_\_\_\_

\_\_\_\_\_  
Signature Date

**HMIS LEAD: City of Springfield Office of Housing**

1600 E. Columbus Ave., Springfield, MA 01103

Name & Title of Authorized Signature: \_\_\_\_\_

\_\_\_\_\_  
Signature Date



## Appendix 2: HMIS User Account Request/Termination Form

DRAFT

**HAMPDEN COUNTY HMIS**  
**HMIS User Account Request Form**

<input type="checkbox"/> New User	<input type="checkbox"/> Delete User	Today's Date: _____
<input type="checkbox"/> Change User Information	<input type="checkbox"/> Other	Effective Date: _____

**Agency Information**

Agency Name: \_\_\_\_\_ Telephone Number: \_\_\_\_\_

Agency Address: \_\_\_\_\_

(Street) (City) (State) (Zip Code)

**Employee (HMIS-User) Information**

Employee Name: \_\_\_\_\_ Telephone Number: \_\_\_\_\_

Employee Title: \_\_\_\_\_ Email: \_\_\_\_\_

Program: \_\_\_\_\_

**Authorization & Confidential Statement**

I agree to maintain strict confidentiality of information obtained through the Hampden County HMIS. Information will be used only for legitimate client services and administration of the employer organization. I agree to abide by all policies and procedures in the Hampden County CoC HMIS Policies and Procedures Manual. I certify that I have completed the online Security and Privacy Training module.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Executive Director's Signature/Authorization

\_\_\_\_\_  
Date

Employee must sign and return the Hampden County HMIS User Agreement along with this request form to the Hampden County CoC HMIS Administrator in order to receive a HMIS User ID and Password. HMIS User must change his/her password upon receipt.

## Appendix 3: Hampden County HMIS User Agreement

DRAFT

## HAMPDEN COUNTY HMIS

### User Agreement

Date: \_\_\_\_\_

User: \_\_\_\_\_

Employee Work Phone Number \_\_\_\_\_ Ext: \_\_\_\_\_

Employee E-Mail Address: \_\_\_\_\_

Agency Name: \_\_\_\_\_

Program Name: \_\_\_\_\_

I understand that I will be allowed access to confidential information and/or records in order that I may perform my specific job duties. I further understand and agree that I am not to disclose confidential information and/or Client records without the prior written consent of my employer, unless such disclosure is required by law.

#### User Responsibilities

Your User ID and Password give you access to data in the Hampden County HMIS. Initial each item below to indicate your understanding and acceptance of the proper use of this access. Failure to uphold the confidentiality standards set forth below is grounds for suspension of HMIS user privileges until such time as the issue is resolved.

\_\_\_\_\_ My User ID and Password are for my use only and must not be shared with anyone.

\_\_\_\_\_ I must take all responsible means to keep my User ID and Password physically secure.

\_\_\_\_\_ I understand that the only persons who may view Client files in the HMIS are authorized users and the Client to whom the information pertains.

\_\_\_\_\_ I may only view, obtain, disclose, or use the database information that is necessary to perform my job and none other.

\_\_\_\_\_ I will not leave a workstation where I am logged into HMIS unattended.

\_\_\_\_\_ I will log off of HMIS before leaving the workstation, even for a short time.

\_\_\_\_\_ I will assure that any printouts/hard copies of HMIS information are properly secured.

\_\_\_\_\_ I will notify my supervisor if I notice or suspect a breach in privacy or security.

## Ethical Data Usage

Once you have completed Security/Privacy training and signed your User Agreement, you are entitled to access to the HMIS. In addition to the responsibilities listed above, you must also adhere to the following principles of ethical data usage.

- Authorized Users will only ask Clients for information necessary to providing services, comply with contractual agreements, and to improve or better coordinate services.
- Authorized Users will ensure that Clients understand that their data is being collected and managed in the HMIS.
- Authorized Users will obtain a signed Release of Information (ROI) form before sharing client data with an outside program or agency on the HMIS.
- Authorized Users will maintain a copy of the ROI Form.
- Authorized Users will not knowingly enter false and/or misleading information into the HMIS.
- Authorized Users will only use data in accordance with the Privacy Policy.

By affixing my signature to this document, I acknowledge that I have been provided a copy of my organization's Privacy Notice and agree to comply with its terms.

---

User Signature

Date

---

Program or Dept. Manager Signature

Date

## Appendix 4: Authorized User List Form

DRAFT

## HAMPDEN COUNTY HMIS

### Authorized User List

**CHO Agency:**

---

**Date:**

---

**Person**

**Submitting Form:**

---

User Name:

---

User Name:

---

User Name:

---

User Name:

---

User Name:

---

User Name:

---

User Name:

---

User Name:

---

User Name:

---

User Name:

---

This form must be completed and submitted every quarter to Deborah Merkman, Hampden HMIS Administrator. Please email the form to [dmerkman@springfieldcityhall.com](mailto:dmerkman@springfieldcityhall.com) or fax it to (413) 787-6515.

*Quarterly due dates are: January 15, April 15, July 15, October 15*

## Appendix 5: Data Collection Forms

- Universal (head or household and household member)
- Program Specific (head of household and household member)
- Interim Assessment
- Exit/Discharge

[Forms to be added.]

DRAFT



## Appendix 6: Interagency Data Network Sharing Agreement

DRAFT

## HAMPDEN COUNTY HMIS

### Interagency Data Network Sharing Agreement

In order to systematically share general client data with other Partner Agencies, interested agencies have jointly established an Interagency Data Network Sharing Agreement (IDNSA) formalized by the execution of this agreement.

This IDNSA is entered into on \_\_\_\_\_ by the Partner Agencies that have signed this agreement. This executed IDNSA shall establish a Data Sharing Network comprised solely of those Participating Agencies that are signatories.

Each Agency listed on the attachment agrees as follows:

#### I. General Understandings

1. In this agreement, the following terms shall have the following meanings:
  - “Client” refers to a consumer of services;
  - “Partner Agency” shall refer generally to any service provider organization which directly enters in the Hampden County HMIS database [or syncs with ASIST?];
  - “Participating Agency” shall refer generally to any service provider organization which participates in this Data Sharing Agreement;
  - “Data Sharing Network” shall refer collectively to all service provider organizations that are participating in this Data Sharing Agreement;
  - “Hampden County HMIS” refers to the Social Solutions ETO System managed by the City of Springfield as the HMIS Lead and adopted by the Hampden County Continuum of Care as the CoC’s official Homeless Management Information System;
  - “HMIS Administrator” refers to the designated individual housed at the City of Springfield Office of Housing who is responsible for overseeing the daily technical aspects of the Hampden County HMIS;
  - “Privacy Notice” shall refer to the standard Hampden County HMIS form, or a comparable form developed by the Agency, which incorporates the content of the standard Hampden County HMIS Privacy Notice;
  - “Client Consent for Release of Information for Data Sharing” shall refer to the standard Hampden County HMIS form or a comparable form developed by the Agency, which incorporates the content of the standard Hampden County HMIS Client Consent for Release of Information for Data Sharing form.
2. The Board-appointed executive officer of each Participating Agency is ultimately responsible for ensuring that users within his/her agency abide by all policies stated in this IDNSA.

3. Only the Agencies which are listed on the attachment and whose executive directors have signed the agreement and dated the signatory page shall be considered a Participating Agency in this Data Sharing Network.
4. Each Participating Agency understands that any additions, subtractions or modifications to the original list of Participating Agencies shall require notification to all remaining Participating Agencies and the HMIS Administrator.

## **II. Authorization**

The HMIS Administrator shall authorize data sharing to begin among a network. Data Sharing shall not begin without authorization from the HMIS Administrator. Authorization shall not be granted until the HMIS Administrator obtains the original copy of this IDNSA, which has been signed and dated by the Executive Director of each Participating Agency.

Each Participating Agency shall retain a copy of this IDNSA.

## **III. Confidentiality**

The Participating Agency shall uphold relevant federal and state confidentiality regulations and laws that protect Client records. The Participating Agency shall only release client records with written consent by the client or the client's guardian, unless otherwise specified in its Privacy Notice.

1. The Participating Agency shall abide specifically with the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and all rules and regulations promulgated pursuant to the authority granted therein (collectively, and collectively with HIPAA, the "HIPAA Regulations" and including, but not limited to, those set forth in 45 C.F.R. §§ 160-164 (2003), all as supplemented, replaced and amended from time to time).
2. The Participating Agency shall abide specifically by federal confidentiality regulations as contained in the Code of Federal regulations, 42 CFR Part 2 regarding disclosure of alcohol and/or drug abuse records. In general terms, the federal rules prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Participating Agency understands the federal rules restrict the use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
3. The Participating Agency will not solicit or input information from clients into the Hampden County HMIS unless it is essential to provide services or perform one of the functions described in the Privacy Notice.

4. The Participating Agency agrees not to release any confidential information received from the Hampden County HMIS database to any organization or individual for the purpose other than those specified in the Privacy Notice without specific written consent by the client.
5. The Participating Agency agrees not to release any client information collected by other Participating Agencies stored within the Hampden County HMIS database to any organization or individual not in this Data Sharing Network, unless specified in the Privacy Notice.
6. The Participating Agency will ensure that all persons accessing the Hampden County HMIS have completed the privacy and security training modules, have executed an Hampden County HMIS User Agreement, and have been issued his/her own User ID and password for the Hampden County HMIS. The Participating Agency will ensure that all persons who are issued a User ID and password for the Hampden County HMIS abide by this IDNSA, including the confidentiality rules and regulations.

#### **IV. Notice and Informed Consent**

Participating Agencies shall use the required client notification and/or consent procedure described in the Policies and Procedures Manual prior to entering any client level data in the Hampden County HMIS.

1. Pursuant to the U.S. Department of Housing and Urban Development Data and Technical Standards Final Notice published in the Federal Register on July 30, 2004 and the Hampden County HMIS policies and procedures, each Participating Agency will prominently display a Data Collection notice at all intake locations and will make available to all clients the Hampden County HMIS Privacy Notice or a notice developed by the Participating Agency that incorporates the content of the Hampden County HMIS Privacy Notice, to all clients enrolling in the Participating Agency programs and services. The Participating Agency will update its Privacy Notice as needed to comply with federal law and regulations and with HMIS policy changes.
2. The Participating Agency shall provide a verbal explanation of the Hampden County HMIS and shall make special accommodations to assist the client in the event that an individual needs special accommodations, is not literate in English or has difficulty understanding the consent form.
3. The Participating Agency will implement the appropriate procedures necessary to enforce the client notification and consent procedures and to ensure that Participating Agency personnel diligently present the Privacy Notice to incoming Clients. The Participating Agency understands that proper notice, as defined by the Policies and Procedures, is required before entering client information into the Hampden County HMIS.
4. The Participating Agency understands that informed written client consent must be received from the client in order to authorize data sharing with other agencies in this Data Sharing

Network. Informed, written client consent shall be documented by completion of the Hampden County HMIS Client Consent for Release of Information for Data Sharing Form.

5. The Participating Agency shall keep signed copies of the Client Consent for Release of Information for Data Sharing forms on file for a period of three years (or specific end date, if client has indicated one) after the completion of the consent timeframe. The Participating Agency shall make copies of the Client Consent available to other Participating Agencies upon request.
6. The Participating Agency shall not knowingly enter false or misleading data under any circumstances.
7. The Participating Agency understands that Clients have the right to refuse to sign the Client Consent - Release of Information for Data Sharing. Services will be provided to Clients regardless of whether the Client agrees to release his or her information for the purpose of interagency data sharing, provided the Client would otherwise be eligible for services.

#### **V. Use of Shared Data by Participating Agencies**

The Participating Agency shall comply with and enforce the User Agreements and the Hampden County HMIS Policies and Procedures. The Executive Director of the Participating Agency is responsible for establishing and monitoring proper procedures for agency staff access to and use of the Hampden County HMIS.

1. The Participating Agency agrees only to allow access to the Hampden County HMIS based upon need. Need exists only for those program staff, volunteers or designated personnel who work directly with clients or who supervise staff working directly with clients and for those program staff, volunteers or designated personnel with data entry or data-related agency administrative responsibilities.
2. User roles shall limit each user's access and ability to modify or delete portions of shared Client information. Each Participating Agency will assign appropriate user access to authorized Agency users based upon their functions.
3. The Participating Agency shall establish business controls and practices to ensure organizational adherence to the Hampden County HMIS Policies and Procedures regarding Interagency Data Sharing.
4. Hampden County HMIS management may implement monitoring procedures to ensure compliance with the requisite Client consent and data sharing procedures as defined by this agreement, the Participation Agreement and the Hampden County HMIS Policies and Procedures. Every User and/or Agency in violation of such protocols may be sanctioned

according to the Policies and Procedures, including but not limited to termination of user rights, termination of agency participation and other legal action.

## VI. Terms and Conditions

1. The parties hereto agree that this agreement is the complete and exclusive statement of the agreement between parties and superseded all prior proposals and understandings, oral and written, relating to the subject matter of this agreement.
2. No Participating Agency shall transfer or assign any rights or obligations without written consent of the other Participating Agencies.
3. This agreement may be terminated by submitting written notice to the Hampden County HMIS Administrator and the Executive Director of all Participating Agencies with 30 days advance notice. However, please note that, during the first six months immediately following system implementation adjustments to the system cannot be accommodated. In the event that an agency withdraws from the data-sharing network, a revised data sharing network listing will be distributed to all remaining Participating Agencies.

**Agency:** \_\_\_\_\_

Address: \_\_\_\_\_

Name & Title of Authorized Signatory: \_\_\_\_\_

\_\_\_\_\_  
Signature Date

**Agency:** \_\_\_\_\_

Address: \_\_\_\_\_

Name & Title of Authorized Signatory: \_\_\_\_\_

\_\_\_\_\_  
Signature Date

**Agency:** \_\_\_\_\_

Address: \_\_\_\_\_

Name & Title of Authorized Signatory: \_\_\_\_\_

\_\_\_\_\_  
Signature Date

**Attachment A**  
**Data Sharing Network Listing**

The following agencies are participants in the Hampden County HMIS Data Sharing Network:

DRAFT

## Appendix 7: Client Consent for Data Sharing

DRAFT



## HAMPDEN COUNTY HMIS

### Client Consent for Release of Information for Data Sharing

When you request or receive services from a participating agency, we collect information about you and your household and enter it into a database system called the Homeless Management Information System (HMIS). This system helps us serve you better, understand homelessness better, and learn if the services we offer are effective at helping people.

**If you give permission**, we can also use this system to share information in HMIS with other local agencies that serve people who are homeless or at risk of homelessness. If you allow us to share data, it will help us:

- Identify other services or programs you may be eligible for;
- Better coordinate services and referrals for you and your household; and
- Reduce the amount of times that you need to provide the same information at intake.

**Information about mental health, substance abuse and HIV status will NOT be shared.**

A list of Partner Agencies is on the back of this form.

HMIS uses many security protections to ensure confidentiality and only Partner Agencies who have signed an Interagency Network Data Sharing Agreement have access.

**You are not required to share your information in order to receive services from this agency.**

#### CLIENT INFORMED CONSENT/RELEASE OF INFORMATION AUTHORIZATION

You have the option to restrict access to personal information that you are providing about yourself and your minor children.

If you DO NOT Want to allow data sharing between agencies, please write "I do not consent," sign and date this section. Otherwise, leave blank.

\_\_\_\_\_  
(Write "I do not consent")

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

☐ **Please treat information about my children age 17 or younger the same as mine.**

\_\_\_\_\_  
Client Name (Please print)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Agency Personnel Name (Please print)

\_\_\_\_\_  
Agency Personnel Signature

\_\_\_\_\_  
Date

This consent will expire three (3) years from the date signed. You may cancel this authorization at any time by written request, but the cancellation will not be retroactive.

## Appendix 8: Sample Data Collection Notice

DRAFT

## **Data Collection Notice**

We collect personal information directly from you for reasons that are discussed in our privacy statement.

We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons.

We only collect information that we consider to be appropriate.

## **Recopilación de Datos**

Recopilamos información personal directamente de usted por las razones que se discuten en nuestra declaración de privacidad.

Podemos ser requeridos recopilar alguna información personal por ley o por las organizaciones que nos dan dinero para operar este programa. Otra información personal que recopilamos es importante para ejecutar nuestros programas, mejorar los servicios para las personas sin hogar, y para comprender mejor las necesidades de las personas sin hogar.

Nosotros solamente recopilamos información que consideramos apropiado.

## Appendix 9: Sample Privacy Notice (English and Spanish)

DRAFT

## Hampden County HMIS

### Privacy Notice

This notice describes how we may use and share information we have about you and how you can access that information.

HMIS is a database that stores information about clients we serve and services we provide. We collect information that is defined in the U.S. Department of Housing and Urban Development's HMIS Data Standards. This notice applies to the Hampden County HMIS.

#### Uses and Disclosures of Your Information

Information you provide...

- Will be entered into the Hampden County HMIS.
- Will be used to improve, provide and coordinate services.
- May be used in relation to payment or reimbursement for services.
- Will be used to make sure that our programs are effective.
- Will be used to prepare statistical reports.

Information you provide about physical or mental health problems will not be shared with other service providers, unless you have authorized it.

Protected Identifying Information (PII) will be shared only if you authorize it or if required by law, or if there is a serious threat to health or safety.

In Massachusetts, PII includes your name, date of birth, social security number, driver's license number, and bank account numbers. We **DO NOT** collect driver's license or bank account numbers!

#### Your Rights

- Your right to receive services will not be affected if you refuse to provide HMIS information.
- You control who your information is shared with. You may allow or refuse to share your information with other service providers.
- You may give written notice to end all privacy and information sharing agreements at any time.
- You may have a copy of this notice.
- You may view your record, have your record corrected, and file a complaint.

## **How to Inspect and Correct your Personal Information**

You may request a copy of your HMIS record. Please submit a verbal or written request to program staff to get a copy. We will explain any information on it that you do not understand.

We will consider your request to correct inaccurate or incomplete personal information. We may delete or fix information that we agree is inaccurate or incomplete.

We may deny your request to inspect your personal information if...

- The information was gathered in reasonable anticipation of legal actions.
- The information would violate a confidentiality agreement.
- Sharing the information would endanger the life or safety of any individual.

If we deny your request we will explain the reason. We will keep a record of the request and the reason it was denied.

## **Data Storage and Disposal**

We dispose of personal information that is not being used **seven** years after it was created or updated. We may remove personal identifiers from the information instead of getting rid of it.

We may keep information longer if required by laws, statutes, regulations or contracts.

.....

For more information contact the supervisor of your program.  
To file a complaint, contact the Hampden County Continuum of Care:

Jesus Arce  
City of Springfield Office of Housing  
1600 E. Columbus Ave.  
Springfield, MA 01103  
(413) 787-6500  
[jarce@springfieldcityhall.com](mailto:jarce@springfieldcityhall.com)

*We have the right to change this notice at any time. This notice is not a legal contract. We accept and consider all questions or complaints regarding the Hampden County Continuum of Care HMIS.*

## **Hampden County HMIS**

### **Notificación de Privacidad**

Este aviso describe cómo podemos utilizar y compartir la información que tenemos sobre usted y cómo usted puede tener acceso a esa información.

HMIS es una base de datos que almacena información acerca de los clientes que servimos y servicios que ofrecemos . Recogemos la información que se define en el Departamento de Vivienda y Estándares de Datos HMIS de Desarrollo Urbano de EE.UU. . Este aviso se aplica a la Provincia HMIS Hampden.

#### **Usos y divulgaciones de su información**

La información que usted proporcione...

- Se introducirán en el condado de Hampden HMIS.
- Se utilizarán para mejorar, proveer y coordinar servicios.
- Puede ser utilizado en relación con el pago o reembolso de los servicios.
- Se puede utilizar para asegurarse de que nuestros programas son eficaces.
- Se utilizará para elaborar informes estadísticos.

La información que usted proporciona acerca de problemas de salud física o mental no será compartida con otros proveedores de servicios, a menos que usted haya autorizado.

Información de identificación protegida (PII) será compartida sólo si usted lo autorice, o si lo requiere la ley, o si hay una amenaza seria a la salud o la seguridad.

En Massachusetts, PII incluye su nombre, fecha de nacimiento, número de seguro social, número de licencia de conducir y números de cuentas bancarias. No recopilamos licencia de conducir o número de cuenta bancaria!

#### **Sus Derechos**

- Su derecho a recibir los servicios no se verá afectado si se niega a proporcionar información HMIS .
- Usted controla que su información es compartida con. Puede permitir o denegar a compartir su información con otros proveedores de servicios.
- Puede dar aviso por escrito a acabar con toda la privacidad y de los acuerdos de intercambio de información en cualquier momento.
- Es posible que tenga una copia de este aviso.
- Usted puede ver su expediente, que su expediente corregido, y presentar una queja.

## **Cómo revisar y corregir su información personal**

Usted puede solicitar una copia de su expediente HMIS. Por favor, envíe una solicitud verbal o por escrito al personal del programa para obtener una copia. Vamos a explicar toda la información en él que usted no entiende.

Consideraremos su solicitud para corregir la información personal inexacta o incompleta. Podemos eliminar o corregir la información que estamos de acuerdo es inexacta o incompleta.

Podemos negar su solicitud para revisar su información personal si...

- La información se recopiló en previsión razonable de acciones legales.
- La información violaría un acuerdo de confidencialidad.
- Compartir la información pondría en peligro la vida o la seguridad de cualquier persona.

Si negamos su petición le explicaremos la razón. Vamos a mantener un registro de la solicitud y la razón por la que fue denegada.

## **Almacenamiento de datos y eliminación**

Disponemos de información personal que no está siendo utilizado siete años después de su creación o actualización. Podemos quitar los identificadores personales de la información en lugar de deshacerse de ella.

Podemos mantener la información por más tiempo si lo requieren las leyes, estatutos, reglamentos o contratos.

.....

Para más información póngase en contacto con el supervisor de su programa.

Para presentar una queja, comuníquese con el Condado de Atención Continua Hampden:

Jesús Arce  
Ciudad de Springfield Oficina de Vivienda  
1600 E. Columbus Avenue.  
Springfield , MA 01103  
(413) 787-6500  
[jarce@springfieldcityhall.com](mailto:jarce@springfieldcityhall.com)

*Tenemos el derecho de cambiar este aviso en cualquier momento. Este aviso no es un contrato legal.  
Aceptamos y consideramos todas las preguntas o quejas con respecto a la Continuidad de Cuidado HMIS del Condado de Hampden.*



## Appendix 10: CHO Security Certification Document

DRAFT

## Hampden County HMIS

### CHO Security Certification

#### Identification of Security Contact

Organization Name

Security Contact

Name

Title

Phone

Email

Security Contact duties include, but are not limited to:

- Annually review the Security Certification document and test the CHO security practices for compliance.
- Using this Security Certification document, certify that the CHO adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time.
- Communicate any security questions, requests, or security breaches to the Hampden County HMIS System Administrator and Security Officer.
- Communicate security-related HMIS information to the organization's end users.
- Complete security training offered by the HMIS Lead.
- Additional duties specified in the HMIS Participation Agreement.

**CHO Security Contact signature indicating understanding and acceptance of these duties:**

---

Signature

Date

Each organization is required to meet the following security requirements. If the requirement cannot be met at the time of the initial certification, you must indicate a date not later than three months after the initial certification by which you will have met the requirement. At that time, you will be required to submit an updated version of this form demonstrating your compliance.

	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
User Authentication	Does the agency abide by the HMIS policies for unique user names and password?	<p>All HMIS users at the agency are aware that they should:</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N NEVER share username and passwords</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N NEVER keep usernames/ passwords in public locations</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N NEVER use their internet browser to store passwords</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N All users have signed a receipt of compliance for staff</p>	
Hard Copy Data	Does agency have procedures in place to protect hard copy Personal Protected Information (PPI) generated from or for the HMIS?	<p>Agency has procedure for hard copy PPI that includes:</p> <p>(1) Security of hard copy files</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Locked drawer/file cabinet</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Locked office</p> <p>(2) Procedure for client data generated from the HMIS</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Printed screen shots</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N HMIS client reports</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Downloaded data into Excel</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Copy of above procedures is available</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Agency trains all staff on hard copy procedures</p>	
PPI Storage	Does the agency dispose of or remove identifiers from a client record after a specified period of time? (Minimum standard: 7 years after PPI was last changed if record is not in current use.)	<p><input type="checkbox"/> Y <input type="checkbox"/> N Agency has a procedure</p> <p>Describe procedure:</p> <p>_____</p> <p>_____</p>	

Virus Protection	Do all computers have virus protection with automatic update? (This includes non-HMIS computers if they are networked with HMIS computers.)	Virus software and version _____ ___ Y ___ N Auto-update turned on  Date last updated: ____ / ____ / ____  Person responsible for monitoring/updating: _____	
Firewall	Does the agency have a firewall on the network and/or workstation(s) to protect the HMIS systems from outside intrusion?	Single computer agencies: ___ Y ___ N Individual workstation  Version: _____  Networked (multiple computer) agencies: ___ Y ___ N Network firewall  Version: _____	
Physical Access	Are all HMIS workstations in secure locations or are they manned at all times if they are in publicly accessible locations? (This includes non-HMIS computers if they are networked with HMIS computers.)	All workstations are: ___ Y ___ N In secure locations (locked ofcs) or manned at all times ___ Y ___ N Using password protected screensavers  All printers used to print hard copies from the HMIS are: ___ Y ___ N In secure locations  Data Access: ___ Y ___ N Users may access HMIS from outside the workplace ___ Y ___ N If yes, Agency has a data access policy	
Data Disposal	Does the agency have policies and procedures to dispose of hard copy PPI or electronic media?	___ Y ___ N Agency shreds all hardcopy PPI before disposal  Before disposal, the Agency reformats/degausses (demagnetizes): ___ Y ___ N Disks ___ Y ___ N CDs ___ Y ___ N Computer hard-drives ___ Y ___ N Other media (tapes, jump drives, etc)	

Software Security	Do all HMIS workstations have current operating system and internet browser security? (This includes non-HMIS computers if networked with HMIS computers.)	Operating System (OS) Version: _____ <input type="checkbox"/> Y <input type="checkbox"/> N All OS updates are installed <input type="checkbox"/> Y <input type="checkbox"/> N Most recent version of Internet Browser(s) are installed	
-------------------	--	--	--

We affirm and certify the above information is true and that this organization, \_\_\_\_\_, is in full compliance with all requirements listed as “CHO” (Contributing HMIS Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the Hampden County HMIS Policies and Procedures or will be in compliance within the timeframes stated above. This certification is incorporated into the HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

HMIS Security Contact

Signature

Date

Executing Officer

Signature

Date