***Appendix G*: SAMPLE NYC HMIS Project End User Agreement**

CHOs are responsible for having all end users of their project-level HMIS compliant home system annually complete and sign an agreement such as this. These agreements must be kept on file by the CHO. End user is defined as any individual that enters or accesses information in the project-level HMIS compliant home system.

End User: _____ (print full name)

End User's title: _____

End User's work phone number: _____

End User's work e-mail: _____

Project(s): _____

Organization: _____

USER POLICY

HMIS Project End Users will comply, to the best of their ability, both with the policies and procedures of their organization and the NYC CCoC HMIS policies and procedures. As guardians entrusted with personal data, [_____] users have a moral and a legal obligation to ensure that the data they
organization name
collect is being collected, accessed and used appropriately, as well as a duty to protect client information. It is also the responsibility of each user to ensure that client data is only used to the ends to which it was collected. Proper user training, adherence to the NYC CCoC Policies and Procedures, and a clear understanding of client confidentiality are vital to achieving these goals.

USER RESPONSIBILITY

Your User ID and Password give you access to [name of project level HMIS compliant system] and data. By signing this form below you indicate your understanding and acceptance of the proper use of this access. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from the system.

Please initial before each bullet point to indicate you have read each statement, understand, and agree.

_____ I understand that each client must be made aware of the CHO's privacy policy (the "Privacy Policy") and its content regarding the collection, use and maintenance of such client's protected personally identifiable information.

_____ I understand that the Privacy Policy must be provided to the client upon request and a notice indicating that the Privacy Policy is available must be posted at the provider's intake desk.

_____ I understand that my User ID and Password are for my use only and will not be shared with anyone.

_____ I will take all reasonable precautions to keep my Password physically secure.

_____ I will never let anyone else know my password, use my Password, or access the system using my password.

_____ I will only let only individuals who are authorized view information in the system (or the Client to whom the information pertains).

_____ I will only view, obtain, disclose, or use the database information that is necessary to perform my job.

_____ I will not leave a computer unattended when I am logged into the system.
_____ I will log-off the system before leaving the work area, even for a very short time.
_____ I understand that failure to log off [name of system] appropriately may result in a breach in client confidentiality.
_____ I will assure that any and all printouts / hard copies of client information must be kept in a secure place, such as a locked file.
_____ I will assure that any printouts / hard copies of client information no longer needed will be shredded or otherwise properly destroyed to maintain confidentiality.
_____ If I notice or suspect a security breach, I will immediately notify my organization HMIS security contact, [name].

I affirm the following:

_____ I have received training in how to use [name of system].
_____ I have will abide by all policies and procedures in the NYC CCoC HMIS Policies and Procedures and have adequate training and knowledge to enter data.
_____ I will maintain the confidentiality of client data as specified in the NYC CCoC HMIS Policies and Procedures.
_____ I will only collect, enter and extract data in [name of system] that is relevant to the delivery of services to persons in the homeless assistance system in New York City.

I, (**Print**) **_____**, acknowledge that I have received the NYC HMIS Policies and Procedures. I understand and agree to comply with the requirements contained in the Policies and Procedures. I further understand that failure to comply with the Policies and Procedures may result in sanctions, up to and including termination and civil and criminal penalties.

I understand and agree to comply with all the statements listed above.

_____

CHO Project End User Signature Date

_____

CHO Supervisor Signature Date

_____

Supervisor's printed name Supervisor's title

***Appendix H*: SAMPLE Minimal Standard CHO Privacy Policy**

Your organization must have a privacy policy with these minimal standards in place. It should be provided to all end-users at your organization prior to their completion of the Project End User Agreement (see Appendix G). Organizations must provide a point of contact for complaints and accountability (see #1 under Complaints and Accountability).

Privacy Policy for _____
(Organization Name)

What this Policy Covers.

1. This document describes the privacy policy and practices of _____. Our main office is at _____.
2. This policy covers the collection, use, and maintenance of protected personal information for clients of _____, as an organization affiliated with the NYC Coalition on the Continuum of Care (CCoC).
3. Personally Identifiable Information/ Protected Identifying Information (PII) is any personal information we maintain about a client that:
    a. Allows identification of an individual directly or indirectly;
    b. Can be manipulated by a reasonably foreseeable method to identify a specific individual; or
    c. Can be linked with other available information to identify a specific client.
4. We adopted this policy because the Department of Housing and Urban Development issued standards for Homeless Management Information Systems. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).
5. This policy informs our clients, our staff, and others how we process personal information. We follow the policy and practices described in this privacy policy.
6. We may amend our policy or practices at any time. Amendments may affect PII that we obtained before the effective date of the amendment.
7. We give a written copy of this privacy policy to any individual who asks for it.
8. We maintain a copy of this policy on our website at _____

How and Why We Collect PII.

1. We collect PII only when appropriate to provide services or for another specific purpose of our organization or when required by law. We may collect information for these purposes:
    a. To provide individual case management;
    b. To produce aggregate-level reports regarding use of services;
    c. To track individual project-level outcomes;
    d. To identify unfilled service needs and plan for the provision of new services;
    e. To conduct research for consulting and/or educational purposes; and
    f. To accomplish any and all other purposes deemed appropriate by the CCoC.

2. We only use lawful and fair means to collect PII.
3. We normally collect with the knowledge or consent of our clients. If you seek our assistance and provide us with PII, we assume that you consent to the collection of information described in this policy.
4. We share this data with the NYC Department of Social Services (DSS), Federal Homeless Policy and Reporting unit (FHPR) a/k/a/ the "HUD CoC unit": the agency appointed by the CCoC to manage all PII we record about our clients. This agency is required to maintain the confidentiality of the data.
5. We post a sign at our intake desk or other location explaining the reasons we ask for PII. The sign says:

   _____

   _____

   _____

   [SAMPLE LANGUAGE; CHOs SHOULD REPLACE THIS LANGUAGE WITH THEIR OWN, AS APPROPRIATE] <*We collect personal information about homeless individuals in a computer system called a Homeless Management Information System (HMIS) for reasons that are discussed in our privacy policy. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless individuals, and to better understand the needs of homeless individuals. We only collect information that we consider to be appropriate. If you have any questions or would like to see our privacy policy, our staff will provide you with a copy.*>

How We Use and Disclose PII.

1. We use or disclose PII for activities described in this part of the policy. We may or may not make any of these uses or disclosures of your PII. We assume that you consent to the use or disclosure of your PII for the purposes described below and for other uses and disclosures that we determine to be compatible with these uses or disclosures:
   a. To provide or coordinate services to individuals;
   b. for functions related to payment or reimbursement for services;
   c. To carry out administrative functions such as legal, audits, personnel, oversight and management functions;
   d. To create de-identified (anonymous) information;
   e. When required by law to the extent that use or disclosure complies with and is limited to the requirements of the law;
   f. To avert a serious threat to health or safety if:
      i. We believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
      ii. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
   g. To report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence in any of the following three circumstances:
      i. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;

ii. If the individual agrees to the disclosure; or

iii. To the extent that the disclosure is expressly authorized by statute or regulation and either of the following are applicable:

A. We believe the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

B. 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;

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

A. We, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm; or

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

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

i. In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

ii. If the law enforcement official makes a written request for PII that:

A. Is signed by a supervisory official of the law enforcement agency seeking the PII;

B. States that the information is relevant and material to a legitimate law enforcement investigation;

C. Identifies the PII sought;

D. Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

E. States that de-identified information could not be used to accomplish the purpose of the disclosure.

iii. If we believe in good faith that the PII constitutes evidence of criminal conduct that occurred on our premises;

iv. 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:

A. 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

B. The information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

i. To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.

j. To third parties for the following purposes:

i. To permit other systems of care to conduct data matches (i.e., to determine if you are also utilizing services from such other systems of care); and

ii. To permit third party research firms and/or evaluators to perform research and evaluation services in connection with the programs administered by the CCoC and the other agencies;

A. Provided that before PII is disclosed under this subsection, the third party that will receive such PII and use it as permitted above must first execute a Data Use & Disclosure Agreement requiring such third party to comply with all applicable laws and regulations, including the privacy standards and disclosure provisions contained in the Department of Housing and Urban Development Homeless Management Information Systems; Data and Technical Standards Final Notice (see 69 Federal Register 45888 (July 30, 2004)), which such standards and provisions are reflected herein.

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

How to Inspect and Correct PII.

1. You may inspect and have a copy of your PII that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete PII that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. We may deny your request for inspection or copying of PII if:
    a. The information was compiled in reasonable anticipation of litigation or comparable proceedings;
    b. The information is about another individual (other than a health care provider or homeless provider);
    c. The information was obtained under a promise of confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information; or
    d. Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
4. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the PII that we maintain, documentation of the request and the reason for the denial.
5. We may reject repeated or harassing requests for access to or correction of PII.

Data Retention.

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

Complaints and Accountability.

1. We accept and consider questions or complaints about our privacy and security policies and practices. You may ask <name an individual or provide a point of contact and describe a process for submitting questions or complaints.>
2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy policy. Each staff member must receive and acknowledge receipt of a copy of this privacy policy.
3. In the event that your question or complaint is not sufficiently addressed through this organization, you may take your concerns to the Grievance Committee of the CCoC. Individuals will submit grievances in writing to the co-chairs. The co-chairs will pass the grievance to the Grievance Committee, which will review it and make a recommendation back to the co-chairs. The co-chairs will make the final decision about the outcome and notify you. More information about this Committee can be found at www.nychomeless.com. Additionally you may take your concerns to the NYC Commission on Human Rights.

***Appendix I*: NYC HMIS Data Standards**

Appendix I is provided as a reference for contributing HMIS organizations and those considering HMIS participation.

Participation in the HMIS requires that you collect all the universal and program-specific data elements on all clients served in your program consistent with the most recent HUD HMIS Data Standards and the requirements of your program funding**.**

HUD's data standards specify the information that must be collected for each project and client, the allowable responses, the frequency with which the information must be updated, and the format in which it can be transferred across data systems, including to the NYC HMIS Data warehouse. HUD's HMIS data standards require that "*An HMIS software must be able to collect all of the data elements defined within this HMIS Data Dictionary, support the system logic, including dependencies, identified in this document, and ensure that the data collection and the visibility of data elements is appropriate to the project type and federal funding sources for any given project*" (HMIS Data Standards Data Dictionary, v. 1.3, p. 2).

The complete HMIS data standards consist of three documents:

- HMIS Data Standards Manual (https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf)
- HMIS Data Standards Data Dictionary (https://www.hudexchange.info/resources/documents/HMIS-Data-Dictionary.pdf)
- HMIS CSV Format Specifications (https://hudhdx.info/Resources/Vendors/5_1_2/HMISCSVSpecifications6_12.pdf)

These materials can be accessed at the following websites:

- https://www.hudexchange.info/resource/3824/hmis-data-dictionary/
- www.NYCHOMELESS.gov

HMIS data is used for project-level performance reporting to HUD, the NYC CCoC evaluation process, and New York City homeless assistance system reporting to HUD.

Appendix J: Sample Security Incident Reporting Form

CHO's must have an agency security incident reporting form to be used in the event of a security incident. At a minimum, it must include the information below. In the event of a security incident, the CHO must report it to the DSS Security Officer & HMIS lead system admin (include names & contacts).

Introduction

On [insert date MM/DD/YYYY], [insert Agency Name] experienced a security incident involving elements of our information technology infrastructure.

Provide a brief, high-level overview of the incident that occurred, what network components were affected, what the expected cause was, what measures were taken, and what the next steps will be. Limited this introduction to a single paragraph.

This report will document the security incident's following details:

- Times, dates, and activities attempted by the Information Technology (IT) department throughout the incident.
- Activities accomplished by the IT department.
- Impact of the incident on IT services and infrastructure.
- Alerting and detection methods used.
- IT's response to the incident.
- Changes made and/or required by IT as a result of lessons learned from the incident.

Timeline and Activities

Use the following table to list information from security log files. Use only those log files that pertain to the incident itself, and include any physical actions taken by IT. Attach all copies of pertinent log files to this report. How many entries are included depends on the length and type of security incident.

Date	Time	Source IP	Target	Protocol	Details

Activities Performed During Incident

Discuss here the historical context of the incident. Include any information derived from the user(s) of the system(s) or device(s) that were compromised.

Example:

- A user may have been traveling for business purposes and using his or her company laptop to log onto the Internet via Wi-Fi connections at several different airports. This would mean that the laptop was connecting without the benefit of the corporate firewall or of updated anti-virus definitions.

- Include what type of worm or Trojan IT believes infected the laptop and how IT has reached this conclusion.

Impact on IT Services

Provide full details on how the security incident impacted IT operations and services, if at all. State if the impact was high, medium, or low, based on the different services, procedures, and devices compromised. In the case of an infected laptop, operational impact on enterprise IT infrastructure would be minimal if the laptop's infection was caught early enough. From a procedural standpoint, however, the impact would be much higher.

Alerting and Detection Methods

State how or by what procedure the security incident was discovered. For instance, the laptop's infection was discovered during a normal review of firewall logs by the network administrator, or via an Intrusion Detection System.

IT's Response to Incident

1. State how long it took for IT to report the incident to senior management.

2. State how long it took to mitigate the security incident. This timeline should span the moment in which the incident was detected until the immediate threat was ended.

Next Steps and Changes Made to Prevent and Solve in the Future

Give a high-level strategic outlook of how IT security must change in order to prevent future threats from occurring. For example, "The IT security perimeter must be altered to prevent unauthorized traffic from leaving the network, such as a Trojan notifying its creator that a back door has been established. This will be enforced by updating egress rules on the corporate firewall."

- "Text":
    - "activity"

- Add any other mitigation techniques to be employed by IT.

Current Status of Incident

Updates

_____

Name of person completing form Date

Title, email, phone, main agency #

_____

Executing Officer (Signature) Date

Name, title, etc..