

HMIS SECURITY &

PRIVACY PLAN

**Three County Continuum of Care**

**PRIVACY & SECURITY**

Privacy refers to the protection of the client's data stored in an HMIS from open view, sharing, or inappropriate use. Security refers to the protection of the client's data stored in the HMIS from unauthorized access, use, or modification.

HMIS Privacy and Security Plan

*Current Version Proposed by the Three County Continuum of Care (September, 2022)*

**Contents**

[Introduction 2](#_Toc113281681)

[Privacy 3](#_Toc113281682)

[Security 5](#_Toc113281683)

[Security Officers 5](#_Toc113281684)

[Security Audit 6](#_Toc113281685)

[Physical Safeguards 7](#_Toc113281686)

[Technical Safeguards 8](#_Toc113281687)

[*Workstation Security* 8](#_Toc113281688)

[Workforce Security 10](#_Toc113281689)

[Reporting Security Incidents 11](#_Toc113281690)

[Disaster Recovery Plan 12](#_Toc113281691)

[APPENDIX A- Three County CoC HMIS – Workstation Privacy and Security Checklist 14](#_Toc113281692)

[APPENDIX B - Community Action Pioneer Valley Clarity HMIS Three County Continuum of Care User Account Request Form 16](#_Toc113281693)

# Introduction

The HMIS Lead Agency is responsible for overseeing HMIS privacy and security. The HMIS Lead Agency may delegate some specific duties related to maintaining HMIS privacy and security to an HMIS System Administrator. The HMIS System Administrator is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the System Administrator’s control and for preventing inadvertent release of confidential client-specific information through physical, electronic or visual access to Administrator workstations. HMIS Partner Agencies are responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency’s control and for preventing inadvertent release of confidential client specific information through physical, electronic or visual access to End User workstations. Each Partner Agency is responsible for ensuring it meets the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards. Partner Agencies will conduct a thorough review of internal policies and procedures regarding HMIS every six months.

If Partner Agencies need support in implementing these Privacy and Security Plans or have any questions or requests related to this these Plans, please contact:

Michele LaFleur, Three County CoC Data & Evaluation Manager: mlafleur@communityaction.us

# Privacy

Each HMIS Partner Agency must have a Privacy Statement that describes how and when the Partner Agency may use and disclose clients’ Protected Personal Information (PPI). PPI includes name, Social Security Number (SSN), date of birth, zip code, project entry and exit date, unique personal identification number (HMIS number) and project identification number.

Partner Agencies may be required to collect some PPI by law, or by organizations that give the agency money to operate their projects. PPI is also collected by Partner Agencies to monitor project operations, to better understand the needs of people experiencing homelessness, and to improve services for people experiencing homelessness.

Partner Agencies are only permitted to collect PPI only with a client’s consent.

Partner Agencies may use and disclose client PPI to:

1. Verify eligibility for services,
2. Provide clients with and/or refer clients to services that meet their needs,
3. Manage and evaluate the performance of programs,
4. Report about program operations and outcomes to funders and/or apply for additional funding to support agency programs,
5. Collaborate with other agencies to improve service coordination

Partner Agencies may also be required to disclose PPI for the following reasons:

1. When the law requires it,
2. When necessary to prevent or respond to a serious and imminent threat to health or safety,
3. When legally required, such as when ordered by a judge, law enforcement or administrative agency

Partner Agencies are obligated to limit disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure.

Uses and disclosures of PPI not described above may only be made with a client’s written consent. Clients have the right to revoke consent at any time by submitting a request in writing.

Clients also have the right to request in writing:

1. A copy of all PPI collected,
2. An amendment to any PPI used to make decisions about care and services (this request may be denied at the discretion of the agency, but the client’s request should be noted in the project records),
3. An account of all disclosures of client PPI,
4. Restrictions on the type of information disclosed to outside partners,
5. A current copy of the Partner Agency’s privacy statement.

Partner Agencies may reserve the right to refuse a client’s request for inspection or copying of their own case files, for example, in the following circumstances:

1. Information compiled in reasonable anticipation of litigation or comparable proceedings,
2. The record includes information about another individual (other than a health care or homeless provider),
3. The information was obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) and a disclosure would reveal the source of the information,
4. The Partner Agency believes that disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If a client’s request is denied, the client should receive a written explanation of the reason for denial. The client has the right to appeal the denial by following the established Partner Agency grievance procedure. Regardless of the outcome of the appeal, the client shall have the right to add to his/her client file a concise statement of disagreement.

All individuals with access to PPI are required to complete formal training in privacy requirements at least annually and is required prior to using the HMIS. This may be accomplished either through an in person training, a virtual training, or by reviewing recordings of the virtual training on the CoC’s Learning Management System.

Partner Agency Privacy Statements may be amended at any time. Amendments may affect information obtained by the agency before the date of the change. An amendment to the Privacy Statement regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. This Privacy Statement must be made available to clients upon request and prior versions may also be available upon request.

This document should, at a minimum, reflect the baseline requirements listed in the HMIS

Data and Technical Standards Final Notice, published by HUD in July 2004 and revised in

March 2010. In any instance where this Privacy Statement is not consistent with the HUD Standards, the HUD Standards take precedence. Should any inconsistencies be identified, please immediately notify the Three County CoC & HMIS Lead Agency, using the contact information below.

If Partner Agencies need support in implementing these Privacy and Security Plans or have any questions or requests related to this Privacy Statement, please contact:

Michele LaFleur, Three County CoC Data & Evaluation Manager: mlafleur@communityaction.us

# Security

## Security Officers

The HMIS Lead Agency and all HMIS Partner Agencies must designate Security Officers to oversee HMIS privacy and security.

### Lead Security Officer

1. May be an HMIS System Administrator or another employee, volunteer or contractor designated by the HMIS Lead Agency who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance,
2. Assesses security measures in place prior to establishing access to HMIS for a new Partner Agency,
3. Reviews and maintains file of Partner Agency annual compliance certification checklists,
4. Conducts annual security audit of all Partner Agencies.

### Partner Agency Security Officer

1. May be the Partner Agency Executive Director or other authorized HMIS signatory, HMIS Agency Manager or Administrator, or another CoC Partner Agency employee, volunteer or contractor, or CoC staff member who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance.
	1. The Partner Agency Security Officer is ideally a staff member of the Partner Agency if the agency has capacity to designate a staff person in this role. If the Partner Agency does not have a staff person who can fill this role, they should reach out to the HMIS System Administrator for help designating another person as the Security Officer for that Partner Agency.
2. Conducts a security audit for any workstation that will be used for HMIS data collection or entry
	1. no less than twice a year for all agency HMIS workstations, AND
	2. prior to issuing a User ID to a new HMIS User, AND
	3. any time an existing user moves to a new workstation.
3. Continually ensures each workstation within the Partner Agency used for HMIS data collection or entry is adequately protected by a firewall (software or hardware) and antivirus software,
4. Completes the HMIS Workstation Privacy & Security Checklist, and forwards the Checklist to the Lead Security Officer.

## Security Audit

### New HMIS Partner Agency Security Assessment

1. Prior to establishing access to HMIS for a new Partner Agency, the Lead Security Officer will assess the security measures in place at the Partner Agency to protect client data (see HMIS Workstation Security & Privacy Checklist – Appendix A). The Lead Security Officer or other HMIS System Administrator will meet with the Partner Agency

Executive Director (Or otherwise authorized HMIS Signatory), Partner Agency HMIS Agency Administrator/Manager(s) and Partner Agency Security Officer to review the Partner Agency’s information security protocols prior to countersigning the HMIS Policies & Procedures Agency Agreement. This security review shall in no way reduce the Partner Agency’s responsibility for information security, which is the full and complete responsibility of the Partner Agency, its Executive Director, and Security Officer.

### Regular Partner Agency Self-Audits

1. The Partner Agency Security Officer will use the HMIS Workstation Security & Privacy Checklist to conduct security audits of all Partner Agency HMIS workstations:
	1. no less than twice a year (not within 3 months unless needed) for all agency HMIS workstations, AND
	2. prior to issuing a User ID to a new HMIS End User, AND
	3. any time an existing user moves to a new workstation.
2. The Partner Agency Security Officer will ensure HMIS users have access to agency computers and that two-factor authentication is set up for logging into the HMIS (when requested). HMIS Users must certify that they will not remotely access HMIS from a workstation (i.e.: personal computer) that is not subject to the Partner Agency Security Officer’s regular audits.
3. If areas are identified that require action due to noncompliance with these standards or any element of the Three County CoC HMIS Policies and Procedures Agency Agreement, the Partner Agency Security Officer will note these on the HMIS Workstation Privacy & Security Checklist and the Partner Agency Security Officer and/or HMIS Agency Administrator/Manager(s) will work to resolve the action item(s) within 15 days.
4. Any HMIS Workstation Privacy & Security Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved. The checklist findings, action items, and resolution summary must be reviewed and signed by the Partner Agency Executive Director or other authorized HMIS Signatory prior to being forwarded to the Lead Security Officer.
5. The Partner Agency Security Officer must turn in a copy of the HMIS Workstation Privacy & Security Checklist to the Lead Security Officer within one week of completion.

### Annual Security Audits

1. The Lead Security Officer will schedule the annual security audit in advance with the Partner Agency Security Officer.
2. The Lead Security Officer will meet with the Partner Agency Security Officer to review completed HMIS Workstation Privacy & Security Checklists from each HMIS Partner Agency. These HMIS Workstation Privacy & Security Checklists must include all agency workstations which access the HMIS. If the Partner Agency Security Officer is not an employee of the Partner Agency, a Program Manager or Executive Level designee such as an authorized HMIS Signatory should be present as well.
3. The Lead Security Officer and the Partner Agency Security Officer (and, if applicable, the Partner Agency non-Security Officer employee) will use part of this meeting to discuss any HMIS privacy and security questions or challenges the Partner Agency may be facing or may need assistance with.
4. If it is deemed necessary by the Lead Security Officer or the Three County Continuum of Care Board of Directors, the Lead Security Officer and the Partner Agency Security Officer will schedule a time for the Lead Security Officer to conduct an audit of at least 30% of HMIS User workstations, with a minimum of 2.
5. If areas are identified that require action due to noncompliance with these standards or any element of the Three County HMIS Policies and Procedures, the Lead Security Officer will note these on the HMIS Workstation Security & Privacy Checklist and the Partner Agency Security Officer and/or HMIS Agency Administrator/Manager(s) will work to resolve the action item(s) within 15 days.
6. Any HMIS Workstation Security & Privacy Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the Checklist findings, action items, and resolution summary has been reviewed and signed by the Partner Agency Executive Director or authorized HMIS signatory and forwarded to the HMIS Lead Security Officer.

## Physical Safeguards

In order to protect client privacy it is important that the following physical safeguards be put in place. For the purpose of this section, authorized persons will be considered only those individuals who have completed Privacy and Security training within the past 12 months.

1. Computer Location – A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The HMIS workstation must not be accessible to clients, the public or other unauthorized Partner Agency staff members or volunteers.
2. Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.

3. PC Access (visual) — Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized Partner Agency staff members or volunteers and utilize visibility/privacy filters to protect client privacy.

## Technical Safeguards

## *Workstation Security*

1. To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations. Approved workstations are technology which were distributed by the agency, include all required security measures, and are subject to Partner Agency Self Audits.
2. Partner Agency Security Officer will confirm that any workstation accessing HMIS shall have antivirus software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly).
3. Partner Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall.

### Establishing HMIS User IDs and Access Levels

1. The Partner Agency Executive Director or other authorized HMIS signatory will ensure that any prospective HMIS User reads, understands and signs the HMIS User Agreement.
2. The Partner Agency Executive Director or other authorized HMIS signatory is responsible for ensuring that all agency HMIS Users have completed HMIS Privacy and Security training prior to being provided with a User ID to access HMIS.
3. All HMIS Users will be issued a unique User ID and password. Sharing of User IDs and passwords by or among more than one HMIS User is expressly prohibited. Each HMIS User must be specifically identified as the sole holder of a User ID and password. User IDs and passwords may not be transferred from one user to another.
4. The Partner Agency Executive Director or other authorized HMIS signatory will always attempt to assign the most restrictive access that allows the HMIS User to efficiently and effectively perform their assigned duties.
5. The Partner Agency Executive Director or other authorized HMIS signatory will submit the New User Request Form for the CAPV Clarity HMIS (Appendix B) to the System Administrator at mlafleur@communityaction.us. This form, along with all of the CoC’s HMIS privacy and security documents, can be found at <https://www.threecountycoc.communityaction.us/hmis> and/or https://www.threecountycoc.communityaction.us/three-county-coc-documents.
6. When the Partner Agency Executive Director or other authorized HMIS signatory determines that it is necessary to change a user’s access level, the Partner Agency Executive Director or other authorized HMIS signatory will submit another New User Request form to Michele LaFleur (mlafleur@communityaction.us) to change the user’s access level as needed and notify the Three County CoC.

### Passwords

1. User IDs are individual and passwords are confidential. No individual should ever use or allow use of a User ID that is not assigned to that individual, and user specified passwords should never be shared or communicated in any format.
2. HMIS Users and Partner Agency Executive Director or other authorized HMIS signatories should indicate on the New User Request Form if they would like 2-Factor Authentication to be utilized for their account.
3. Temporary passwords must be changed on first use. User-specified passwords must be a minimum of 8 characters long and must contain a combination of letters and at least two numbers.
4. HMIS users will be prompted by the software to change their password every 180 days.
5. If HMIS Users cannot remember their password, they can reset their password from the Clarity HMIS login page by clicking on “Forgot password?” HMIS Users will then be asked to enter their email address and will be sent an email with a “Reset Password” button which will allow users to change their password. This “Reset Password” button is available for 60 minutes before it expires.
6. User accounts will be automatically locked after 180 days with no log in. To unlock an account, a request must be placed with the System Administrator at (mlafleur@communityaction.us)
7. HMIS Users must immediately notify their Partner Agency Executive Director or Security Officer if they have reason to believe that someone else has gained access to their password.
8. Four consecutive unsuccessful attempts to login will disable the User ID until the password is reset. To unlock an account, a request must be placed with the System Administrator at (mlafleur@communityaction.us)

### Rescinding User Access

1. The Three County CoC, through Michele LaFleur (mlafleur@communityaction.us), should be notified within 24 hours if an HMIS User no longer requires access to perform his or her assigned duties due to a change of job duties or termination of employment in order to deactivate their accounts in the Three County CoC Clarity HMIS and/or the Data Warehouse.
2. In the event of suspected or demonstrated noncompliance by an HMIS User with the HMIS End User Agreement or any other HMIS or data warehouse plans, forms, standards or governance documents, the Partner Agency Executive Director or other authorized HMIS signatory or Security Officer should notify the Three County CoC. The User ID for the HMIS User in question in both the HMIS and the Data Warehouse will be deactivated by the Three County CoC until an internal agency investigation has been completed. The Partner Agency Executive Director or other authorized HMIS signatory or Security Officer shall notify the Three County CoC of any substantiated incidents that may have resulted in a breach of Data Warehouse or HMIS system security and/or client confidentiality, whether or not a breach is definitively known to have occurred.
3. In the event that the Three County CoC suspects potential noncompliance by an HMIS User, the Three County CoC is empowered to deactivate User IDs in the HMIS and the Data Warehouse pending further investigation.
4. The Three County Continuum of Care is empowered to permanently revoke a Partner Agency’s access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Three County CoC HMIS Policies and Procedures Agency Agreement, or the Partner Agency Privacy Statement that resulted in a release of Personal Protected Information (PPI). The Three County CoC is empowered to permanently revoke a Partner Agency’s access to the Three County CoC Data Warehouse for substantiated noncompliance with the provisions of these Security Standards, the Three County CoC HMIS Policies and Procedures Agency Agreement, or the Partner Agency Privacy Statement that resulted in a release of Personal Protected Information (PPI).

### Other Technical Safeguards

1. The Lead Security Officer shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.
2. The Partner Agency Security Officer shall develop and implement procedures for managing new, retired, and compromised local system account credentials.
3. The Partner Agency Security Officer shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks.
4. Unencrypted PPI may not be stored or transmitted in any fashion—including sending file attachments by email or downloading reports including PPI to a flash drive, to the End User’s desktop or to an agency shared drive, aside from password protected documents which may be used to transmit PPI if all other security protocols are followed and the recipient is authorized to view that client PPI. All downloaded files containing PPI must be deleted from the workstation temporary files and the “Recycling Bin” emptied before the End User leaves the workstation.

## Workforce Security

The HMIS Lead Agency will ensure background checks are conducted on any individual to be designated as a Lead Security Officer or HMIS System Administrator. Partner Agencies will ensure background checks are conducted on any individual to be designated as a Partner Agency Security Officer.

1. The results of the background check must be considered on a case-by-case basis, with the goal of protecting the security and integrity of the HMIS system and safeguarding the personal information contained therein. An individual whose background indicates that they may not sufficiently be relied upon to help achieve this goal may not be given administrative-level access to HMIS.
2. The results of the background check must be retained in the subject’s personnel file.

For Partner Agency Security Officers, the Partner Agency must forward to the Lead Security Officer a document certifying that a background check was conducted and that the Agency believes the individual to be capable of advancing the goal of protecting the security and integrity of the HMIS system and safeguarding the personal information contained therein.

1. A background check may be conducted only once for each person unless otherwise required.

## Reporting Security Incidents

These Security Standards and the associated Three County HMIS Policies and Procedures are intended to prevent—to the greatest degree possible—any security incidents. However, should a security incident occur, the following procedures should be followed in reporting:

1. Any HMIS User who becomes aware of or suspects that HMIS system security and/or client privacy has been compromised must immediately report the concern to their Partner Agency Security Officer.
2. In the event of a suspected security or privacy concern the Partner Agency Security Officer should complete an internal investigation. If the suspected security or privacy concern resulted from an HMIS User’s suspected or demonstrated noncompliance with the HMIS End User Agreement, the Partner Agency Security Officer should reach out to the system administrator (mlafleur@communityaction.us) to request the HMIS User’s account be deactivated until the internal investigation has been completed.
3. Following the internal investigation, the Partner Agency Security Officer shall notify the Lead Security Officer of any substantiated incidents that may have compromised HMIS system security and/or client privacy whether or not a release of client PPI is definitively known to have occurred. If the security or privacy concern resulted from demonstrated noncompliance by an HMIS User with the HMIS End User Agreement, the Lead Security Officer reserves the right to permanently deactivate the User ID for the HMIS User in question.
4. Within 1 business day after the Lead Security Officer receives notice of the security or privacy concern, the Lead Security Officer and Partner Agency Security Officer will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent such future concerns. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed 30 days.
5. If the Partner Agency is not able to meet the terms of the action plan within the time allotted, the HMIS Lead, in consultation with the Three County Continuum of Care Board, may elect to restrict or temporarily terminate the Partner Agency’s access to HMIS. The Partner Agency may appeal to the Three County CoC Board for reinstatement to HMIS following completion of the requirements of the action plan.
6. In the event of a substantiated release of Personal Protected Information (PPI) in noncompliance with the provisions of these Security Standards, the Three County CoC HMIS Policies and Procedures Agency Agreement, or the Partner Agency Privacy Statement, the Partner Agency Security Officer will make a reasonable attempt to notify all impacted individual(s). The Lead Security Officer must approve of the method of notification and the Partner Agency Security Officer must provide the Lead Security Officer with evidence of the Agency’s notification attempt(s). If the Lead Security Officer is not satisfied with the Agency’s efforts to notify impacted individuals, the Lead Security Officer will attempt to notify impacted individuals at the Agency’s expense.
7. The HMIS Lead Agency will notify the appropriate body of the Continuum of Care of any substantiated release of Personal Protected Information (PPI) in noncompliance with the provisions of these Security Standards, the Three County HMIS Policies and Procedures, or the Partner Agency Privacy Statement.
8. The HMIS Lead Agency will maintain a record of all substantiated releases of Personal Protected Information (PPI) in noncompliance with the provisions of these Security Standards, the Three County HMIS Policies and Procedures, or the Partner Agency Privacy Statement for 7 years.
9. The Continuum of Care reserves the right to permanently revoke a Partner Agency’s access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Three County CoC HMIS Policies and Procedures Agency Agreement, or the Partner Agency Privacy Statement that resulted in a release of Personal Protected Information (PPI).

## Disaster Recovery Plan

Disaster recovery for the Three County Continuum of Care HMIS will be conducted by the HMIS System Administrator with support from the HMIS software vendor. The HMIS System Administrator must be familiar with the disaster recovery plan set in place by the HMIS software vendor.

1. The HMIS System Administrator should maintain ready access to the following information:
	1. Contact information – Phone number and email address of the software vendor contact person responsible for recovering the Continuum of Care’s data after a disaster.
	2. HMIS System Administrator responsibilities – A thorough understanding of the HMIS System Administrator’s role in facilitating recovery from a disaster.
2. All HMIS System Administrators should be aware of and trained to complete any tasks or procedures for which they are responsible in the event of a disaster.
3. The HMIS System Administrator must have a plan for restoring local computing capabilities and internet connectivity for the HMIS System Administrator’s facilities.

This plan should include the following provisions.

* 1. Account information – Account numbers and contact information for internet service provider, support contracts, and equipment warranties.
	2. Minimum equipment needs – A list of the computer and network equipment required to restore minimal access to the HMIS service, and to continue providing services to HMIS Partner Agencies.
	3. Network and system configuration information – Documentation of the configuration settings required to restore local user accounts and internet access.

# APPENDIX A- Three County CoC HMIS – Workstation Privacy and Security Checklist

Note: This form should be completed for each workstation used for HMIS.

 HMIS User Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Workstation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| 1.  | Password-protected login “Does the primary work station for each HMIS User require a unique, password-protected login?”  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □ Fully compliant with policy □ May be brought into compliance within 30 days with minor corrections □ Non-compliant with policy |
| 2.  | Password-protected screensaver after five minutes “Does the primary work station for each HMIS User activate a screensaver after five minutes of inactivity, and require a password to exit the screen saver and access the work station?”  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □ Fully compliant with policy □ May be brought into compliance within 30 days with minor corrections □ Non-compliant with policy  |
| 3.  | Operating system updated at least weekly “Is the operating system on the primary work station for each HMIS User updated at least weekly, either manually or through automatic system updates?”  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □ Fully compliant with policy □ May be brought into compliance within 30 days with minor corrections □ Non-compliant with policy |

|  |  |
| --- | --- |
| 4.  | Protected by a firewall“Is the primary workstation for each end user protected by a firewall, blocking unsolicited and unauthorized connections to and from the system?”  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □ Fully compliant with policy □ May be brought into compliance within 30 days with minor corrections □ Non-compliant with policy |
| 5.  | Using Firefox 91, Chrome 92, Safari 14, Microsoft Edge or later “Is the primary workstation for each End User equipped with Firefox 91, Chrome 9, Safari 14, Microsoft Edge or a later version of these browsers? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □ Fully compliant with policy □ May be brought into compliance within 30 days with minor corrections □ Non-compliant with policy |
| 6.  | Weekly scan for viruses and malware “Is the primary workstation for each end user equipped with anti-virus/anti-malware software and scanned at least weekly for viruses and malware?”  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □ Fully compliant with policy □ May be brought into compliance within 30 days with minor corrections □ Non-compliant with policy |
| 7.  | Data Collection notice appropriately displayed “Is the required Data Collection Notice prominently displayed wherever data collection typically takes place?”  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □ Fully compliant with policy □ May be brought into compliance within 30 days with minor corrections □ Non-compliant with policy |

# APPENDIX B - Community Action Pioneer Valley Clarity HMIS Three County Continuum of Care User Account Request Form

New User [ ]  Coordinated Entry Access [ ]  **Today’s Date:**\_\_\_\_\_\_/\_\_\_\_/\_\_\_\_\_\_\_\_\_

Delete User [ ]  Change User Access Role [ ]

**Access Level Requested:** Staff [ ]  Administrator [ ]  Manager [ ]

**HMIS User Information**

First Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Last Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Agency/Organization: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Job Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Phone Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Background Check Statement**

Pursuant to 24 CFR 580.35(d)(2) relating to the HMIS security standards, the user listed above has successfully passed a criminal background check conducted by the user organization and is eligible to access HMIS.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized Signature (CEO/Executive Director/Signatory) Printed Name Date

**Authorization & Confidentiality Statement**

My agency agrees to maintain strict confidentiality of information obtained through HMIS. This information will be used only for the legitimate client services and administration of the above named organization/agency. I understand that it is the responsibility of the Partner Agency Executive Director, or authorized HMIS signatory, to notify the HMIS System Administrator of the user's termination from the agency, placement on disciplinary probation, or upon any change in duties not necessitating access to HMIS information within one business day of the occurrence.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized Signature (CEO/Executive Director/Signatory) Printed Name Date

***If requesting CES Access, this form requires additional signature from the CoC Coordinated Entry Specialist or Homeless Services Coordinator.***

User has completed necessary Coordinated Entry Assessor and HMIS training and is authorized to access the Coordinated Entry System program within HMIS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized Signature Printed Name Date

(CoC Coordinated Entry Specialist or Homeless Services Coordinator)

**Access Level Descriptions**

**Staff: Can create and edit client records, program enrollments, assessments, services, notes, files, attendance, household management, location, contacts, and referrals. Can also access client history and run reports in the report library.**

**Administrator: Everything included in the staff level, plus the ability to delete services, enrollments, files, notes, location, contacts, assessments, and referrals. Also is able to restore deleted data.**

**Manager (No more than 1 per agency): Everything included in the Administrator level, plus the ability to access the ‘Manage’ screen which allows users to edit, add, or delete services, programs, sites, funding sources, and more. Also gives the ability to manage staff accounts and audit their HMIS usage. It is recommended that HMIS Managers check with the System Administrator before making changes to programs or services. Because of the higher cost of Manager level accounts, the CoC does not have enough to appoint a Manager to each Agency and will be distributed on a first come basis and a waitlist. If there are staff on the waitlist, Manager accounts which become inactive will be reassigned to the first person on the list at that time.**