Alameda County HMIS

Agency/Jurisdiction Implementation Readiness Checklist

□ 1) Two copies Agency/Jurisdiction Partner MOU signed & mailed

□ 2) HMIS Policies & Procedures Manual copy printed for Agency use

□ 3) Agency/Jurisdiction Privacy Notice completed and copy submitted to HMIS staff

□ 4) Agency/Jurisdiction Staff all sign Agreement acknowledging receipt and compliance with Privacy Notice; notify HMIS

□ 5) Agency/Jurisdiction Privacy Notice *Sign* Posted

□ 6) Agency/Jurisdiction Privacy Notice Posted on Website (if applicable)

□ 7) Agency/Jurisdiction Client Consent (ROI) Form Received

□ 8) Agency/Jurisdiction Restricted Data Release Form Submitted (□ not applicable)

□ 9) Agency/Jurisdiction Workstation "Collection" *Signs* Posted

□ 10) Agency/Jurisdiction Intake and Exit Forms Completed (□ Supplemental created)

□ 11) Privacy Certification Training Completed for All Staff

□ 12) Workflow assessed and modified to support Privacy Standards

□ 13) Technical Readiness Completed; Forms Submitted
(firewall, anti-virus, workstation screensaver w/password)

□ 14) HMIS software licensed Users Identified

□ 15) Provider Assessment(s) Completed and Submitted

Signature & Date certifying completion of the above: ___________________________________

To return documents identified in this checklist: Email to hmissupport@acgov.org or fax to 510.670.6378

If you have any questions about any checklist items: Contact support at hmissupport@acgov.org.

□ Agency/Jurisdiction Partner MOU Signed

Agency MOU Signed

1.0 Agency/Jurisdiction MOU Policy – Alameda County HMIS Policies and Procedures.

Each participating agency/jurisdiction must have a signed Memorandum of Understanding (MOU) with EveryOne Home to use the HMIS system and must be compliant with the terms of the MOU to continue use of HMIS.

□ Agency/Jurisdiction Privacy Notice completed and copy submitted to HMIS staff

1. HMIS staff provided each agency with an electronic copy of a sample Agency Privacy Notice.

2. Each agency/jurisdiction will need to send a copy of their completed Agency Privacy Notice to HMIS staff.

Agency Privacy Notice Completed

2.3 Notification of Privacy Protections Policy – Alameda County HMIS Policies and Procedures.

Each participating agency/jurisdiction will document all privacy protections in its Privacy Notice document.

4.2.4. Openness – HUD HMIS Privacy and Security Standards.

A CHO must publish a privacy notice describing its policies and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request.

□ Agency/Jurisdiction Staff all sign Agreement acknowledging receipt and compliance with Privacy Notice

1. Each agency/jurisdiction will need to send a signed letter to HMIS staff indicating each of their staff (as defined below by HUD) has signed such an agreement with the agency/jurisdiction.

Agency Staff all sign Agreement acknowledging receipt and compliance with Privacy Notice

4.2.6. Accountability – HUD HMIS Privacy and Security Standards.

A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice

□ Agency/Jurisdiction Privacy Notice Sign Posted

1. The agency/jurisdiction can use the electronic sample provided or the language in the Privacy and Security Training manual for compliance with this signage.

2. A sign must be posted at each physical location at which the agency/jurisdiction provides services.

Agency Privacy Notice Sign Posted in Agency

4.2.4. Openness – HUD HMIS Privacy and Security Standards.

A CHO must post a sign stating the availability of its privacy notice to any individual who requests a copy.

□ Agency/Jurisdiction Privacy Notice Posted on Website (if applicable)

1. If the agency/jurisdiction qualifies under this standard, the agency/jurisdiction must send an email to HMISSupport@acgov.org with the web address of the website and link to the posted Privacy Notice.

Agency Privacy Notice Posted on Website (if applicable)

4.2.4. Openness – HUD HMIS Privacy and Security Standards.

If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page.

□ Agency/Jurisdiction Client Consent (ROI) Form

1. HMIS staff will send a sample electronic version of the Agency Client Consent (ROI) form to each agency/jurisdiction to review. If you decide to use the standard form, a final PDF version with your agency's name will be sent to you.

2. If you are going to incorporate this form into a current agency form, you must send a final version of that "incorporated" form to HMIS staff.

Agency Client Consent (ROI) Form

3.0 Decision to Participate Policy – Alameda County HMIS Policies and Procedures.

Clients have the right to specify if their personal information may be shared in the HMIS system. Clients can not be refused services if they choose not to share the Intake in HMIS.

(F) If a client chooses to share Intake data, the client will sign the “Client Release of Information Authorization” form. This form must be “witnessed” in writing by an agency/jurisdiction representative.

□ Agency/Jurisdiction Restricted Data Release Form

1. If your agency/jurisdiction has situations in which it will need to release restricted data from the HMIS system (as listed in the following paragraph) to other entities, it must have a Restricted Data Release Form specifically for this purpose.

2. A copy of this Restricted Data Release form must be faxed or emailed to HMIS staff.

Agency Restricted Data Release Form

HMIS Client Consent – Alameda County HMIS Policies and Procedures.

While collected for all programs, NO medical, HIV/AIDS, mental health, substance use, details about a disability, or any violence-related information will be shared outside of this agency unless you provide express written consent on a separate form.

□ Agency/Jurisdiction Workstation “Collection” Signs Posted

1. For compliance with this standard, the agency/jurisdiction can use the language in italics below, or the sample sign located in the Privacy and Security Certification Training folder. The language for the signs will also be available electronically to agency/jurisdictions.

2. A sign containing this language must be posted at each intake desk (or comparable location) at each physical location where the agency/jurisdiction conducts the intake process.

Agency Workstation “Collection” signs posted

3.0 Decision to Participate Policy – Alameda County HMIS Policies and Procedures.

4.2.6. Accountability – HUD HMIS Privacy and Security Standards.

A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information.

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."

□ Agency/Jurisdiction Intake and Exit Form Completed

1. HMIS staff will provide each agency/jurisdiction with the HMIS Standard ADULT and Standard CHILD Intake Forms (SIFs), Exit Form, and Permanent Housing Status Change form. Each agency/jurisdiction must collect the data fields contained in these forms.
2. If your agency/jurisdiction is producing a customized version of the HMIS Standard ADULT and Standard CHILD Intake Forms (SIFs), you will need to send a copy of each customized SIF version to HMIS staff.

Agency Intake and Exit Form completed

Agency/jurisdictions may customize the HMIS Standard ADULT and Standard CHILD Intake Forms (SIFs). However, every question on the HMIS SIFs (ADULT and CHILD) must be included in any customized agency form.

The Program Exit form that is used for all programs cannot be modified except to add questions the agency/jurisdiction may want to ask at Program Exit.

The order of the questions on the HMIS Forms reflects the order of data entry fields in the HMIS software. Changing the order of questions on your customized agency form may make data entry more difficult for your agency/jurisdiction.

□ Privacy Certification Training Completed for all staff

1. All identified staff or designees identified to participate in privacy training have completed the course and been certified.

Privacy Training Completed

7.0 Privacy and Security Policy – Alameda County HMIS Policies and Procedures.

Any agency/jurisdiction staff or designees conducting any intake, data entry, or other data processing functions must complete Privacy and Security Certification Training and become certified. Upon initial implementation of
an agency/jurisdiction, Privacy and Security Certification Training will be provided by HMIS staff. All subsequent Privacy and Security Certification Training of new agency/jurisdiction staff for the HMIS system will be completed by either attending an HMIS-sponsored Certification Training or by one-on-one training sessions conducted by the agency/jurisdiction's HMIS manager or Policy and Procedure Administrator using HMIS-provided Training and Certification module and materials. The HMIS Privacy and Security Certification Trainings, conducted by HMIS staff, will occur regularly, and will be open to all new agency/jurisdiction staff.

□ Workflow assessed and modified to support Privacy Standards

1. Your agency/jurisdiction must review all workflow process and procedures that involve PPI intended for or produced from the HMIS system to insure it supports adherence to all HMIS standards for which the agency/jurisdiction is responsible.

Insure Workflow Supports Adherence to Privacy Standards

Privacy and Security Training / Agency's Role – Alameda County HMIS.

Your agency is responsible for making sure that the flow of PPI within the agency, from Intake, to data entry, to reporting, supports the adherence to all privacy standards protecting client privacy and confidentiality.

□ Technical Readiness
(firewall, anti-virus, workstation screensaver with password)

1. Your agency/jurisdiction must complete an Agency Network System Report form and submit it as indicated on the form.

2. Your agency/jurisdiction must complete an Agency Workstation Checklist form and submit it as indicated on the form.

3. If your agency/jurisdiction plans to access the HMIS software from a workstation outside of your physical primary location network, your agency/jurisdiction must complete an Agency Remote Access Request form and submit it as indicated on the form.

Technical Readiness
(firewall, anti-virus, workstation screensaver w/password, surge protector)

4.3.1. System Security – HUD HMIS Privacy and Security Standards.

FIREWALL: 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.

Technical Readiness (continued)
(firewall, anti-virus, workstation screensaver w/password, surge)

4.3.1. System Security – HUD HMIS Privacy and Security Standards.

ANTI-VIRUS: 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.

PHYSICAL ACCESS: 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 are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals.

PASSWORD PROTECTED SCREEN SAVER: After eight minutes of inactivity, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by a CHO.

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.

SURGE SUPPRESSOR: All network servers, workstations, and laptops used to access/collect data for HMIS system must be connected to a surge suppressor.

□ HMIS software Licensed Users Identified

1. Your agency/jurisdiction must complete a <u>HMIS software License Information</u> form and submit it as indicated on the form.

HMIS software Licensed Users Identified

4.0 Issuing of User Licenses Policy – Alameda County HMIS Policies and Procedures.

The HMIS System Administrator will issue all initial agency/jurisdiction user licenses, IDs, and passwords for system users upon completion of software certification and training.

To return documents identified in this checklist:

Email them to hmissupport@acgov.org or fax to 510.670.6378