Protecting Client Confidentiality for Volunteers and Agency Staff

Goals & Objectives

- To understand how the Consent to Share Protected Personal Information Form is used, and what it means.
- To learn how to protect client confidentiality.

Consent to Share Protected Personal Information Form

- Consent to Share Protected Personal Information forms should be available for clients to sign when they complete an intake into your project.
- By signing a Consent to Share Protected Personal Information Form, the client is agreeing to share their Protected Personal Information (PPI) with other agencies participating in HMIS.
- Each agency is responsible for obtaining and storing consent forms for their clients.
- PPI should not be shared with agencies not participating in HMIS.
- The client has the right to receive services, even he/she refuses to sign the Consent to Share Protected Personal Information Form.
- The client has the right to revoke his/her consent by submitting a written request or by completing the Revocation of Consent Form. The client's PPI is then no longer shared with other agencies in HMIS.

Consent to Share Protected Personal Information Form

GREATER LOS ANGELES & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

CONSENT TO SHARE PROTECTED PERSONAL INFORMATION

The LA/OC HMIS is a local electronic database that securely record information (data) about clients accessing housing and homeless services within the Greater Los Angeles and Orange Counties. This organization participates in the HMIS database and shares information with other organizations that use this database. This information is utilized to provide supportive services to you and your household members.

What information is shared in the HMIS database?
We share both Protected Personal Information (PPI) and general information obtained during your intake and assessment, which may include but is not limited to:

- Your name and your contact information

Protecting Client Confidentiality

- Clients' Personal Information should be protected and confidential.
- It is the agency's responsibility to ensure the following practices are implemented to protect client confidentiality.

How to Protect Client Confidentiality

- Install anti-virus and firewall protection on your computer.
  - Agencies must maintain anti-virus software on all PC's on their network. The anti-virus should automatically download updated virus definitions and take precautionary steps and prevent "adware" and "spyware".
- Do not share your computer username and password.
  - You should be required to enter a password when you first log into your computer. This password should not be shared.
- Do not send unencrypted data across a public network.
  - This means any documents with client identifying information must be encrypted and password protected before being sent over email. No unencrypted PPI can ever be sent over email, including but not limited to clients' first or last names, DOB, or SSN.
- Prevent unauthorized individuals from viewing data on your computer screen.
  - The contents of your computer screen should not be visible to clients or visitors that may be at your agency.
- Do not leave computer screen unattended.
  - You should lock your computer screen any time you leave your desk. You should also have a timed screen saver that requires a password for re-entry into your computer.

How to Protect Client Confidentiality

- Store client identifying information in a locked filing cabinet or office.
  - If any documents with client identifying information/PPI have been printed, they should be kept locked in a cabinet or office. This includes any documents with any client PPI such as intake or exit forms, consent forms, identification materials, or other documents related to the client's case.
- Shred printed copies of documents with client's identifying information, if they are not going to be saved in a locked filing cabinet or office.
  - This includes any reports with client PPI that have been printed.
- Do not discuss confidential information without consent from the client.

Questions

- All forms discussed in this training are available at **OCHMIS.org** under **HMIS Help.**

- To see a list of the agencies participating in HMIS, please click here.

- Please direct any questions to your HMIS Agency Administrator or Back-up Agency Administrator, and they can forward your question to the HMIS helpdesk.