Santa Maria/ Santa Barbara County HMIS Security & Privacy

Presenter: Bob Russell
Community Technology Alliance

Why Security & Privacy Matters

Trust

In order to help your client, you will need to ask them many questions, some personal and confidential. Your clients needs to trust their information will be used for their benefit.

Vulnerability

Your client's history may make them suspicious and access to their data often raises legitimate safety concerns.

Collaboration

HMIS is a shared system. Meaning most data entered can be seen by other Agencies (unless that data is locked down). A shared system allows Agencies to exchange data in order to collaboratively assist your client.

HMIS & PPI
(Personal Protected Information)

General PPI

Name

Date of Birth (Age)

Citizenship

Veteran Status

Disability Status

Contact Information
(address, phone, email)

Sensitive PPI

Social Security Number

Driver's License

Medical Records
(including mental health & substance abuse)

Educational Records

Financial Information

Release of Information (ROI)

Client data may only be entered in HMIS if the client has provided informed consent, as demonstrated by a signed ROI.

The ROI is good for 3 years.

Each Agency must attempt to reach a client at least once per year to order to have the client re-sign their ROI.

If a client does not re-sign the ROI for 3 consecutive years, that client is assumed to be no longer active in HMIS.

Your client has the right to have a copy of their ROI and HMIS data.

The ROI (English and Spanish versions) is located in User Central.

Security – Physical Access

If you are authorized to use HMIS, you will be provided a username and password. Do not share these with anyone else.

You will need to change your password every 45 days. Create a robust password.

You will be locked out of HMIS if you enter your password incorrectly 3 consecutive times. Use the Help Desk to request your account be unlocked.

HMIS is to be accessed inside a secure facility (example: your office)

Only Outreach workers (or those authorized to do so) may access HMIS in the field.

If you print something with PPI, secure that document.

Security – Electronic Access

Access HMIS via a secured connection.

If you have been authorized to access HMIS in the field (example: Outreach Worker), use only a secured wireless connection. Do not use public wifi. If your wifi connection does not require a username/password, then that connection is likely public.

Immediately log out of HMIS when done.

Privacy – Client Data

HMIS data is used for providing and evaluating the delivery of housing and housing related services

Aggregate HMIS data is used to provide HUD and other funders with data on the nature and scope of homelessness, and to provide data on the effectiveness of your community's homeless services.

The data you enter in HMIS is shared with other Agencies unless:

- The data is locked down
- There is no ROI or the ROI is expired.

Sharing data with outside entities requires:

- A valid warrant
- The expressed written permission of the client