SECURITY CONFIDENTIALITY

These points need to be communicated to the users:

All users must have their own unique user ID.

You must never use another user’s ID, or allow anyone else to use your User ID.

User passwords should never be shared and should never be communicated in any format.

You are not allowed to write down your password and leave it under your keyboard.

You are not allowed to write down your password and leave it under your pencil drawer.

You may write down your password and keep it under lock and key that only you have access to.

When communicating about a record in the HMIS, like asking to edit a record, use the client ID number, never the clients name.

The computer used to enter data into the HMIS system must be in a non-public area and all efforts must be taken to ensure that the screen is not seen by clients or other coworkers.

You are not allowed to look at records in the HMIS system of clients you have no legitimate business reason to access. Even if you feel it would be in the best interest of your client. You may not “fish around”. The system records every record and every page you access in the system. You can be held legally responsible for your actions in the HMIS system.

By law a client may request documentation of everyone who has accessed his or her information from the HMIS system.

In the event a client requests this report the user should contact their Agency HMIS Administrator who will contact the HMIS Administrator.

Because this report could become a document in a legal action the HMIS System Administrator will do a preliminary investigation to justify all sharing events on the report. If it is determined that a breach of confidentiality may have taken place a more in-depth investigation will be implemented.

Please send signed or filled out forms to ss_HMISsupport@co.slo.ca.us
Points to discuss – pose the question and let the user’s explain to each other how to do that in the HMIS system.

If a client does not want any information about him or her to be shared how should you proceed? __________________________________________________________

______________________________________________________________________

If a client is HIV positive and signs the release “yes, except for anything related to my HIV status”, how do you lock the specific page that contains that information so it can never be released to any other agency? ______________________________________

______________________________________________________________________

If a client signs the release but stipulates no information is to be shared with CAPSLO how should you proceed? __________________________________________

______________________________________________________________________

FYI: If a client wants a copy of all the information entered about him/her into the HMIS system by law we must provide it to him or her. There is a report in the system you can use to show him or her or print out for him or her. If you print it out please make it clear to the client that he or she is responsible for the security of that information.

The following should be handed out to, and filled out by, the user. We need to collect these and keep them on record that they got the information and promise to abide.

Please send signed or filled out forms to ss_HMISsupport@co.slo.ca.us
Agency HMIS Administrator’s need to go over all the presented information with any user that did not attend and have them complete a form as well.

**COMPLIANCE ASSESSMENT**  
Updated September 2019

**Agency: ____________________________**

**Name: ____________________________**

I use only my own assigned User Name when signing onto the HMIS system. ___

I maintain a secure location for the equipment I use to access the HMIS system. ___

I use a locking screen saver. ___

The computer I use to access the HMIS system has virus protection installed and running with automatic updates. ___

The computer I use to access the HMIS system has individual or network firewall protection. ___

I have not nor will I ever post the web site for the HMIS system to any public forum. ___

I have received the County’s HMIS Policies and Procedures manual and agree to abide by it. ___

I maintain a challenging password to help protect the HMIS data. ___

I understand that I will not discuss anything from HMIS with anyone else. ___

**Signature: ____________________________**

Please send signed or filled out forms to ss_HMISsupport@co.slo.ca.us