SACRAMENTO STEPS FORWARD

2023 HMIS ANNUAL SECURITY AUDIT CHECKLIST

Agreements, Certifications & Licenses		
1.	Signed HMIS Partner Agency Agreement	Confirm your agency has a signed copy of this document.
2.	Signed HMIS Staff Verification of HMIS Access	Please conduct a spot check on 5 of your active users to confirm you have these documents. (For agencies with 50+ active users, please sample 10% of them.)
3.	Reviewed the SSF HMIS Privacy and Security Plan	Confirm your agency has reviewed this document.
4.	HMIS Responsible Staff	Please provide us with at least one individual who is your lead HMIS contact(s) for any questions regarding staff or programs.
5.	Agency Security Officer	Please provide us with at least one lead person who knows about your agency's security efforts.

Privacy: Consumer Notice		
There are two kinds of notices, depending on your agency's funding: HUD-Funded or Non-HUD Funded.		
6.	Consumer Notice, posted publicly for client or consumer viewing	The notice should be posted in your lobby or intake offices. Field staff should also carry a copy.
7.	Locations of postings	We will need a brief description of location of the notice, include the addresses where appropriate.
8.	Consumer Notice, posted on Agency website	If the notice is not on your website, please contact your IT Department or webmaster to have it added.
9.	Website link to the Consumer Notice	We will need to know where on your agency website the Consumer Notice is located.
10.	SSF provided Consumer Notice	Confirm your agency has read the notice.
11.	Customized Consumer Notices	Review & edit the notice to include all necessary components to customize it for your agency. Then submit a copy to SSF.
12.	Clients presented with Consumer Notice when requested	Confirm that there are extra copies of this document for clients in your office or you have the ability to print copies if they are requested. Field staff should carry extra copies if requested. All staff should be trained to provide copies to consumers/clients.

Privacy: Hard Copy Data		
13.	Protect hard copy data from unauthorized viewing or access	Ensure client files are not left unattended when not in use and their names are not in plain sight of non-essential personal.
14.	Files are locked in a drawer/file cabinet	Complete a spot check of areas where files are located to make sure drawers are locked.
15.	Offices are locked when not occupied	Complete a spot check of both individual offices and main offices to make sure they are locked.
16.	No visible client files or reports on unoccupied desks or workspaces	Complete a spot check of all unoccupied desks and/or offices.

SACRAMENTO STEPS FORWARD

2023 HMIS ANNUAL SECURITY AUDIT CHECKLIST

Privacy: Hard Copy Data		
13.	Protect hard copy data from unauthorized viewing or access	Ensure client files are not left unattended when not in use and their names are not in plain sight of non-essential personal.
14.	Files are locked in a drawer/file cabinet	Complete a spot check of areas where files are located to make sure drawers are locked.
15.	Offices are locked when not occupied	Complete a spot check of both individual offices and main offices to make sure they are locked.
16.	No visible client files or reports on unoccupied desks or workspaces	Complete a spot check of all unoccupied desks and/or offices.

Computer Systems: Virus Protection and System Updates		
17.	Virus protection with automatic updates	Make sure all computers have automatic updates for their virus protection. If you are unsure, check with your IT Department.
18.	Virus software name, versions, last update	Provide us with the name of your anti-virus software, the version you are using, and the last time it was updated.
19.	Operating System (OS) updates	Make sure all computers, tablets, and mobile devices have automatic updates for their operating system. To manually check for updated operating system, please follow these instructions: • Windows or MacOS (Apple) (for computers) • Android or iPhone/iPad (tablets or phones)

Computer Systems: Firewall		
20.	Firewall to protect internal network servers and local user computers	For individual computers, the firewall can be part of the anti-virus software. For networked systems, the firewall is usually where the internet enters your system. The firewall protection can be a subscription, a service from your internet provider, or it can be incorporated in your router. Check with your IT Department to confirm your security.
21.	Software information for individual workstations	Provide us with the name and version of your firewall software. Check with your IT Department to review your anti-virus software.
22.	Software information for networked systems	Provide us with the name and version of your firewall software. Check with your IT Department to review your anti-virus software.

Computer Systems: Physical Access		
23.	Workstations in secured locations (locked offices)	Do a spot check on 10% of the workstations to ensure compliance.
24.	Workstations are logged off when not in use	Do a spot check on 10% of the workstations to ensure compliance.
25.	Workstations are password protected	Do a spot check on 10% of the workstations to ensure compliance.
26.	Workstations are never used on open Wi-Fi networks (i.e., internet cafes, libraries, airports)	Do a spot check on 10% of the workstations and/or interview 10% of your staff to ensure compliance.
27.	Written plan for remote access	Make sure the agency has a plan for remove access if applicable.