HMIS Quarterly Checklist

HMIS Partner Agency Name:				Security Officer Name:
Q1 - July ☐	Q2 - Oct. ☐	Q3 - Jan. ☐	Q4 - April ☐	Date:

Workstation Security Standards

This Compliance Certification Checklist is to be completed quarterly by the Partner Agency Security Officer for the HMIS Partner Agency named above. Every agency workstation used for HMIS data collection, data entry or reporting must be evaluated. Attach additional copies of any page of this checklist as needed. Any compliance issues identified must be resolved within 30-days. Upon completion, a copy of this checklist should be forwarded to the Lead Security Officer at the HMIS Lead Agency. This original checklist should be readily available on file at the HMIS Partner Agency for 7 years.

For the purpose of this section, authorized persons will be considered only those individuals who have completed HMIS Privacy and Security training within the past 12 months.

1. A Privacy Notice is visibly posted at the HMIS workstation (where applicable).
2. HMIS workstation computer is in a secure location where only authorized persons have access (applies to remote and on-site workers).
3. HMIS workstation computer is password protected and locked when not in use.
4. Documents printed from HMIS are sent to a printer in a secure location where only authorized persons have access.
5. Non-authorized persons are unable to see the HMIS workstation computer monitor.
6. HMIS workstation computer has antivirus software with current virus definitions (within the last 24 hours) and a full system scan within the past week.
7. HMIS workstation has and uses a hardware or software firewall.
8. Unencrypted Protected Personal Information (PPI) has not been electronically stored or transmitted in any fashion (hard drive, flash drive, email, etc.).
9. Hard copies of PPI (client files, intake forms, printed reports, etc.) are stored in a secure location.
10. Password is kept physically secure.

#	Workstation Location or End User Name	1	2	3	4	5	6	7	8	9	10	Notes/Comments
1		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
3		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
4		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
5		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
6		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
7		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
8		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
9		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
10		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

#	Workstation security compliance issues	Steps taken to resolve workstation security compliance issue

Data Quality Standards

1. Combined quarterly Data Quality Report submit to HMIS Lead agency on time
2. For all data elements, the rate of Don't Know/Refused/Missing is less than the established 5% per the Sonoma HMIS Data Quality Plan
3. All Program Descriptor Data Elements are complete and accurately reflect program contracts and operations

#	HMIS Program Name/ID#	1	2	3	If program is not meeting standard, steps being taken to achieve compliance
1		☐	☐	☐	
2		☐	☐	☐	
3		☐	☐	☐	
4		☐	☐	☐	
5		☐	☐	☐	

Security Officer Certifications

(Initials) I have verified that:

_____ All agency End Users are using the most current version of the HMIS ROI and HMIS Partner Agency list.

_____ All agency End Users have signed the End User Agreement, and I maintain a file of all of those signed agreements.

_____ All agency End Users have completed Privacy and Security training within the past 12 months.

_____ All agency End Users require access to HMIS to complete their assigned duties.

_____ _____ _____ _____

Partner Agency Security Officer Signature *Date* *Executive Director (or other empowered officer) Signature* *Date*