Appendix B: Quarterly Compliance Checklist

SANTA CLARA COUNTY HMIS QUARTERLY COMPLIANCE CERTIFICATION CHECKLIST	☐ Quarter 1	HMIS Partner Agency Name :	
	☐ Quarter 2		
	☐ Quarter 3	Security Officer Name:	
	☐ Quarter 4	Date:	

Workstation Security Standards

In partnership with Santa Clara County, Clarity Human Services Software, a division of Bitfocus, Inc., administers the County's Homeless Management Information System ("HMIS"), a shared database software application which confidentially collects, uses, and releases client-level information related to homelessness in the County. Client information is collected in the HMIS and released to nonprofit housing and services providers (each, a "Partner Agency," and collectively, the "Partner Agencies"), which use the information to improve housing and services quality. Partner Agencies may also use client information to identify patterns and monitor trends over time; to conduct needs assessments and prioritize services for certain homeless and low-income subpopulations; to enhance inter-agency coordination; and to monitor and report on the quality of housing and services. This Compliance Certification Checklist is to be completed and certified quarterly by the Partner Agency Security Officer for the HMIS Partner Agency named above according to the schedule outlined below. Each Agency workstation used for HMIS data collection, data entry, or reporting must be certified compliant. Any identified compliance issues must be resolved within thirty (30) days. Upon completion, the original signed copy of this checklist should be retained in the records of the HMIS Partner Agency named above for a minimum of seven (7) years. Additionally, a copy should be made available the SCC Bitfocus System Administration team (the "Lead Security Officer") at Clarity Human Services Software, a division of Bitfocus, Inc.

Compliance Certification Schedule:

- Quarter 1 (due by April 30th): New HMIS users or workstations created in Q1 (Jan-Mar)
- Quarter 2 (due by July 31st): New HMIS users or workstations created in Q2 (Apr-June)
- Quarter 3 (due by October 31st): New HMIS users or workstations created in Q3 (July-Sep)
- Quarter 4 (due by January 31st): ALL Active HMIS Users and Workstations

Checklist Items

1. An HMIS Privacy Statement is visibly posted at each HMIS intake desk (or comparable location). If the workstation is not in a fixed location HMIS Privacy Statement must be provided as a handout.
2. Each HMIS workstation computer is in a secure location where only Authorized Persons * have access.
3. Each HMIS workstation computer is password-protected and locked when not in use. (Changing passwords on a regular basis is recommended)
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 view any HMIS workstation computer monitor.
6. Each HMIS workstation computer has antivirus software with current virus definitions (i.e., within the past twenty-four (24) hours), and each HMIS workstation computer has had a full system scan within the past week.

7. Each HMIS workstation computer has and uses a hardware or software firewall.
8. Unencrypted protected personal information ("PPI") ** has not been electronically stored or transmitted in any fashion (including, without limitation, by hard drive, flash drive, email, etc.). (Encrypted hard drives are recommended)
9. Hard copies of PPI (including, without limitation, client files, intake forms, printed reports, etc.) are stored in a physically secure location.
10. Each HMIS workstation computer password information, including each Authorized Person's user identification information, is kept electronically and physically secure.

**An "Authorized Person" means a Partner Agency authorized agent or representative (an "HMIS End User," or simply an "End User") who has completed the SCC HMIS Client Consent training within the past twelve (12) months.*

*** Protected Personal Information ("PPI") is defined as client-level identifying information, including, without limitation, information about names, birth dates, gender, race, social security number, phone number, residence address, photographic likeness, employment status, income verification, public assistance payments or allowances, food stamp allotments, or other similar information*

Security Officer Workstation Checklist

Instructions: For each HMIS workstation at your agency fill in the workstation location or end username. Verify items 1 through 10 on the previous page for the workstation and check (✓) the box to confirm the verification is complete. Fill in additional notes/comments and compliance issues as needed. Attach additional pages if necessary.

Return this form to scc-admin@bitfocus.com

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

10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												
22												

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

Security Officer Certifications

(Initials) I have verified that:

_____ Each End User is using the most current versions of the Santa Clara County HMIS Client Consent to Data Collection and ROI and the Partner Agency list.

_____ Each Partner Agency End User has been instructed to read and sign the Santa Clara County HMIS End User Agreement, which is viewed electronically in Clarity Human Services the first time a user logs into the system.

_____ Each Partner Agency End User has completed Santa Clara County HMIS Client Consent Training within the past twelve (12) months.

_____ Each Partner Agency End User requires access to HMIS to perform her or his assigned duties.

_____ _____ _____/____/_____

Partner Agency Security Officer Name	*Partner Agency Security Officer Signature*	*Date*