SANTA CLARA COUNTY HMIS

QUARTERLY COMPLIANCE CERTIFICATION CHECKLIST

SELF CERTIFICATION FORM

|  |  |
| --- | --- |
| Staff Name: |  |
| Workstation Location: |  |
| HMIS Partner Agency Name: |  |
| Date Completed: |  |

**Instructions:** Use this form to Self-Certify that you meet the SCC HMIS Workstation Security Standards below at your workstation. This form should be completed and submitted to your agencies’ Security Officer for review.

|  |  |  |
| --- | --- | --- |
| # | Staff Initials | Workstation 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” is 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*

**ADDITIONAL NOTES (including workstation security compliance issues identified and steps taken to resolve):**

|  |
| --- |
|  |

**Additional User Certifications**

|  |  |
| --- | --- |
| (staff initials) |  |
| \_\_\_\_\_\_\_\_ | I am using the most current versions of the Santa Clara County HMIS Client Consent to Data Collection and ROI and the Partner Agency list. (available on the HMIS website <http://scc.hmis.cc/>) |
| \_\_\_\_\_\_\_\_ | I have read and signed 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. |
| \_\_\_\_\_\_\_\_ | I have completed Santa Clara County HMIS Client Consent Training within the past twelve (12) months. |
| \_\_\_\_\_\_\_\_ | I am requires access to HMIS to perform my assigned duties. |

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_/\_\_\_\_/\_\_\_\_\_***

***Staff Name Staff Signature Date***