

KING COUNTY HMIS SEMI-ANNUAL COMPLIANCE CERTIFICATION CHECKLIST

| | | |
|---|--|------------------------|
| HMIS Partner Agency Name: | | Security Officer Name: |
| Semi-Annual: July <input type="checkbox"/> | Semi-Annual: January <input type="checkbox"/> | Date: |

Workstation Security Standards

In partnership with King 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 semi-annually by the Partner Agency Security Officer for the HMIS Partner Agency named above. 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.

For the purposes of the following Workstation Security Standards, “Authorized Person” means a Partner Agency authorized agent or representative (each, an “HMIS End User,” or simply an “End User”) who has completed HMIS Privacy and Security training within the past twelve (12) months.

1. An HMIS Privacy Statement is visibly posted at each HMIS workstation.
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”) – 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 – 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.

SEMI-ANNUAL COMPLIANCE CERTIFICATION CHECKLIST | 6-2-17

| # | 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 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 King 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 King 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 King County HMIS Privacy and Security 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*

Partner Agency Executive Director Name *Partner Agency Executive Director Signature* *Date*