**  
Annual HMIS Site Data Quality and Security Review**

Agency Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Programs Included in Review: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Review Date:

Agency Representative: Print Agency Staff Name, Title, email

TCHC HMIS Representative: TCHC HMIS Security Officer Name, email

Follow up Visit Required: Yes No Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*This signature that the Agency follows required HMIS security and privacy policies and procedures to protect the accuracy and privacy of information stored on persons seeking and receiving services within the Fort Worth/Arlington/Tarrant County Continuum of Care. All issues and concerns identified in this review were addressed to the satisfaction of the HMIS Administration.*

*Please attach all relevant Agency Policies and Procedures related to Client Confidentiality and Data Security to this review for documentation in the TCHC HMIS Administration files.*

Review Approved by: TCHC HMIS Security Officer Signature Date

Review Approved Date: TCHC Executive Director Signature Date

**HMIS Site Data Quality and Security Check-In**

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Description** | **Assessment** | **Action Needed** |
| **Agreements & Certifications** | **Does the agency have a signed copy of their most recent agency Participant Agreement?**  **All user have signed user License Agreements on file.**  **All users have completed applicable training (and have documentation of training**  **All users have completed annual training.** | **Agency:**  \_\_Y \_\_N Has Copy of agency Participant Agreement.  **HMIS Users:**  \_\_Y \_\_N Signed User License Agreements.  \_\_Y \_\_N Completed applicable training.  \_\_Y \_\_N Completed annual training.  \_\_\_\_\_\_\_ % staff attended Annual ETO / HMIS Refresher Training |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Description** | **Assessment** | **Action Needed** |
| **Data Collection** | **The Agency collects all HUD required Universal Data Elements within the HUD Intake.**  **The Agency collects all HUD and CoC required Program Specific Data Elements within the HUD Intake, Mid Program and Exit Assessments.** | **Agency:**  \_\_Y \_\_N Has a data collection protocol  \_\_Y \_\_N Is within HUD’s Acceptable Data Error Guidelines  **ONLY applicable to Federal Partner Programs (e.g., PATH, RHY, SSVF, etc. )**  \_\_Y \_\_N Is capturing Program Data Elements on all clients |  |
| **Data Quality Checks.** | **Agency staff regularly run reports to verify data quality and completeness. Staff correct data quality errors in a timely manner.** | |  | | --- | | \_\_Y \_\_N Agency Security Officer/staff regularly run quarterly data quality reports |   \_\_Y \_\_N Agencies are updating grant and program setups at least annually –  \_\_Y \_\_N Staff regularly correct data entry errors and missing program elements –  \_\_Y \_\_N Un-exited client reports are monitored quarterly  \_\_Y \_\_N Staff run outcome reports as applicable for program type (**only applies to ESG and CoC funded programs – funding source may be found in Project Descriptors)** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Description** | **Assessment** | **Action Needed** |
| **Release Of Information** | Does the agency use appropriate release of information and are they consistent in collecting with clients?  Agency uses the CoC HMIS standardized ROI applicable to its level of sharing? | \_\_Y \_\_N the agency does use appropriate release of information and are they consistent in collecting with clients.  . |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Description** | **Assessment** | **Action Needed** |
| **User Authentication** | **Does the agency abide by the HMIS policies for unique user names and passwords?** | \_\_\_\_\_ % Of Agency’s Active ETO Users are employed, and authorized users by the Agency.  \_\_Y \_\_N All agency HMIS users have a unique user name, password and agency email address.  Number of HMIS users at the agency aware and abide by the HMIS policies they should:  \_\_\_ / \_\_\_\_ Share username and passwords    \_\_\_ / \_\_\_\_ Keep usernames/passwords in public locations  \_\_\_ / \_\_\_\_ Keep store passwords in Internet browser |  |
| **Hard Copy Data** | **Does the agency have procedures in place to protect hard copy Personal Protected Information (PPI) generated from or for the HMIS?** | Agency has procedure for secure use and storage of hard copy Client PPI that includes:  \_\_Y \_\_N All Client (current and former) files are locked in a drawer/file cabinet  \_\_Y \_\_N All Client (current and former) files are locked in an office |  |
| **Requirement** | **Description** | **Assessment** | **Action Needed** |
| **Security Officer.** | **The Agency has a designated Security Officer.** | \_\_Y \_\_N The Agency has a designated Security Officer.  Security Officer Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| **Virus Protection** | **Do all computers have virus protection with automatic update?**  ***(This includes non-HMIS computers if they are networked with HMIS computers.)*** | \_\_Y \_\_N Visual / hands on Inspection of at least 25% of agency computers for ant-virus installation  Agency staff (or contractor) and contact information responsible for monitoring/updating Software installations for the Agency:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Virus software and version:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Software Date last updated \_\_\_\_/\_\_\_\_/\_\_\_\_ |  |
| **Firewall** | **Does the agency have a firewall on the network and/or workstation(s) to protect the Agency computers, servers and other locations of Client and HMIS data?** | Single computer agencies:  \_\_Y \_\_N Individual workstation  Version:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Network (multiple computer) agencies:  \_\_Y \_\_N Network firewall  Version:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Description** | **Assessment** | **Action Needed** |
| **Physical Access** | **Are all HMIS workstations in secure locations or are they manned at all times if they are publicly accessible locations?**  ***(This includes non-HMIS computers if they are networked with HMIS computers.)*** | All workstations are:  \_\_Y \_\_N In secure locations (locked offices) and /or manned at all times  \_\_Y \_\_N Using password-protected screensavers for unique user-logins    All printers used to print hard copies from the HMIS are:  \_\_Y \_\_N In secure locations    Data Access:  \_\_Y \_\_N Users may access HMIS outside the workplace  \_\_Y \_\_N If yes, Agency has a data access policy (Attach hard copy of Agency Policy) or Describe Policy: |  |
| **Data Disposal** | **Does the agency have policy and procedures to dispose of hard copy PPI or electronic media?** | \_\_Y \_\_N Agency shreds all hardcopy Personal Identifying Information before disposal. (Visual inspection of shredder location(s) or outsourced shredding company procedure.)  Before disposal, the Agency reformats Client data to:  \_\_Y \_\_N CDs  \_\_Y \_\_N Computer hard-drives  \_\_Y \_\_N Other media (tapes, jump drives, etc.) |  |
| **Software Security** | **Do all HMIS workstations have current operating system and internet browser security?**  ***(This includes non-HMIS computers if networked with HMIS computers.)*** | Operating System (OS) Version: (Windows XP, 7, 8, 10 etc.)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_Y \_\_N All OS updates are installed  \_\_Y \_\_N Most recent version of Internet Browser(s) are installed (IE 9+) |  |