



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: _____ Date _____

The HMIS Site Review will receive a score that will be incorporated into the Renewal Project Scorecard used for the CoC Competition.

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	<p>Does the agency have a signed copy of their most recent agency Participant Agreement?</p> <p>All user have signed user License Agreements on file.</p> <p>All users have completed applicable training (and have documentation of training)</p> <p>All users have completed annual training.</p>	<p>Agency:</p> <p>Has Copy of agency Participant Agreement:</p> <p>HMIS Users:</p> <p>Signed User License Agreements:</p> <p>Completed applicable training.</p> <p>Completed annual training. *</p> <p>NA % staff attended Annual ETO / HMIS Refresher Training</p>	

Requirement	Description	Assessment	Action Needed
Data Collection	<p>The Agency collects all HUD required Universal Data Elements within the HUD Intake.</p> <p>The Agency collects all HUD and CoC required Program Specific Data Elements within the HUD Intake, Mid Program and Exit Assessments.</p>	<p>Agency:</p> <p>Has a data collection protocol:</p> <p>Is within HUD's Acceptable Data Error Guidelines.*</p> <p><u>ONLY applicable to Federal Partner Programs (e.g., PATH, RHY, SSVF, HOPWA etc.)</u></p> <p>NA -- Is capturing Program Data Elements on all clients.*</p>	

Data Quality Checks.	Agency staff regularly run reports to verify data quality and completeness. Staff correct data quality errors in a timely manner.	<p>Agency Security Officer/staff regularly run quarterly data quality reports</p> <p>Agencies are updating grant and program setups at least annually –</p> <p>Staff regularly correct data entry errors and missing program elements *</p>	
-----------------------------	--	---	--

Requirement	Description	Assessment	Action Needed
Release Of Information	<p>Does the agency use appropriate release of information and are they consistent in collecting with clients?</p> <p>Agency uses the CoC HMIS standardized ROI applicable to its level of sharing?</p>	<p>__Y __N the agency does use appropriate release of information and are they consistent in collecting with clients.</p>	

Requirement	Description	Assessment	Action Needed
User Authentication	Does the agency abide by the HMIS policies for unique user names and passwords?	<p>Are all Agency's ETO users authorized.</p> <p>All agency HMIS users have a unique user name, password and agency email address.</p> <p>Does Agency electronic security policies address:</p> <p>Sharing username and passwords</p> <p>Storing usernames/passwords in public locations</p> <p>Storing passwords in Internet browser</p>	
Hard Copy Data	Does the agency have procedures in place to protect hard copy Personal Protected Information	<p>Agency has procedure for secure use and storage of hard copy Client PPI that includes:</p>	

	(PPI) generated from or for the HMIS?	All Client (current and former) files are locked in a drawer/file cabinet 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.	The Agency has a designated Security Officer. Security Officer Name: Email: Phone:	
Virus Protection	Do all computers have virus protection with automatic update? <i>(This includes n-HMIS computers if they are networked with HMIS computers.)</i>	__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	<p>Are all HMIS workstations in secure locations or are they staffed at all times if they are publicly accessible locations?</p> <p><i>(This includes n-HMIS computers if they are networked with HMIS computers.)</i></p>	<p>All workstations are:</p> <p>In secure locations (locked offices) and /or staffed at all times</p> <p>Using password-protected lock-screens for unique user-logins</p> <p>All printers used to print hard copies from the HMIS are:</p> <p>In secure locations</p> <p>Data Access:</p> <p>Users may access HMIS outside the workplace</p> <p>NA If , Agency has a data access policy (Attach hard copy of Agency Policy) or Describe Policy:</p>	
Data Disposal	<p>Does the agency have policy and procedures to dispose of hard copy PPI or electronic media?</p>	<p>Agency shreds all hardcopy Personal Identifying Information before disposal. (Visual inspection of shredder location(s) or outsourced shredding company procedure.)</p> <p>Before disposal, the Agency reformats Client data to:</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N CDs</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Computer hard-drives</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Other media (tapes, jump drives, etc.)</p>	
Software Security	<p>Do all HMIS workstations have current operating system and internet browser security?</p> <p><i>(This includes n-HMIS computers if networked with HMIS computers.)</i></p>	<p>Operating System (OS) Version: (Windows XP, 7, 8, 10 etc.)</p> <p>Windows 7, Internet Explorer 9+</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N All OS updates are installed</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N Most recent version of Internet Browser(s) are installed (IE 9+)</p>	

*These items will t be included in the 2016 CoC scoring competition. However, they *may* be included in 2017.