DSHS Data Management and Security Risk Assessment Tool

This tool ensures adherence to DSHS HIV/STD data management and security policies and procedures.

Instructions: Respond to each item below for the monitoring period since the last security risk assessment.

Date of Security Risk Assessment: __________

Person Completing the Assessment: ______________________________________

Contractor: __________________________________ **Contract #**: ______________

Item	Item Description	Met	Not Met	N/A	Comments
1	A Local Responsible Party (LRP) has been designated for all matters concerning data management and security.	□	□	□	
2	HIV/STD data management and security policies are in place and available to staff.	□	□	□	
3	All personnel with access to confidential information (including IT staff) have signed confidentiality statements on file and are updated annually.	□	□	□	
4	All personnel with access to confidential information (including IT staff) have received initial data security training as well as an annual update.	□	□	□	
5	Compliance with data security protocols is part of employee performance reviews.	□	□	□	
6	The LRP maintains a list of authorized users with access to confidential data.	□	□	□	
7	Confidential data are: • Maintained in a secured area • Confidential documents are not left in plain sight • Shredded before disposal • Clearly marked as containing confidential information.	□	□	□	
8	Access to the secured area where confidential data is kept is limited to those approved by the LRP.	□	□	□	
9	Confidential data is stored on stand-alone computers or on a secure drive of computers on a secure network.	□	□	□	

Item	Item Description	Met	Not Met	N/A	Comments
10	Computers with confidential information have power-on and screensaver passwords.	□	□	□	
11	Any confidential data taken out of the building secured area are: • Minimized to the essential data required • Stored on devices that are kept secure • Encrypted	□	□	□	
12	Any confidential data transmissions to DSHS or other approved partners are encrypted and transmitted via secured means.	□	□	□	
13	Requests for data are: • Handled according to the established Release of HIV/STD Data policy • Tracked in a data request log • Data release agreements signed when necessary	□	□	□	
14	Staff reported, investigated, and followed up on all suspected breaches according to policy.	□	□	□	
15	Program compliance with established data management and security policies is periodically reviewed by management or the LRP.	□	□	□	

Actions to be completed by DSHS:

Actions to be completed by Contractor: