Data Security and Confidentiality Tool - 2

DATA SECURITY AND CONFIDENTIALITY
INITIAL ASSESSMENT

This checklist can be used to guide the initial assessment of a program’s compliance with the Standards for Data Security and Confidentiality. This will be particularly useful for state and local public health programs that currently lack data security and confidentiality policies and procedures.

As indicated previously in this document, the initial assessment should be conducted by a team led by the ORP(s). The team should include:

Program managers, directors, or equivalent leaders from participating programs

Other representatives of participating programs

Staff members with technical expertise in data security

IT staff

The initial assessment should include the following steps:

* Identify key individuals and designate an ORP
* Review current security-related materials (e.g., written policies and procedures)
* Review relevant state and local laws that might affect data security and confidentiality policies
* Identify any policies or procedures that are either barriers to information sharing or sources of data security weaknesses
* Consult standard operating procedures (SOPs) from other programs that might be useful sources of ideas or suggestions for procedural changes
* Review any history of data security breaches or near-breaches, and associated lessons learned
* Assess physical security and define the secure area
* Assess electronic security protections and methods of data transfer and storage
* Assess factors related to security of information in the field, as appropriate
* Assess training needs

|  |
| --- |
| Conducting an Initial assessment: Steps and Guiding Questions |
| Identify key individuals and designate an ORP | Have key individuals, including program managers, directors, persons responsible for information and system security, and appropriate technical staff members, been identified?Has an ORP(s) with ultimate decision-making authority and responsibility for reconciling differences in policies and procedures across programs been identified? |
| Review current policies and gather resources | Have relevant policies, data-sharing agreements, and standard operating procedures been compiled and reviewed?Have relevant laws, rules, and regulations been considered? |
| Identify weaknesses and barriers  | Have areas of weakness and specific topics that need additional clarification been identified?Have barriers to data sharing been identified?Have potential solutions to these barriers, including possible policy revisions, been noted? |
| Assess physical security and define the secure area | What is the work-space configuration?What is the path of public health data from collection and entry into the program’s physical space through data entry and storage?What happens to case report forms received from providers? How are case report forms completed by health department staff handled? Is information obtained by phone or other electronic format? If so, how are hard copies or electronic media physically secured? Are electronic devices used, such as PDAs or laptops? If so, how are these physically secured?How is the area that houses identifiable data secured? Who has access to the physical space, who needs access, and for what purpose?  |
| Assess electronic security, protections, and methods of data transfer and storage | Who or what roles need access to identifiable data? At what stage is their access required? Who needs access to electronic databases with identifiable data?Who needs access only to de-identified or analysis data sets?Who teleworks and what level of access do they need? Are electronic protections in place for remote access?Which individuals must take identifiable information in the field or outside of the secure physical area or health department? How is that information brought back into the office and what happens when it arrives? Does field work involve information on paper or electronic data on laptops or other storage devices?What electronic protections are in place during data transfer? Is encryption used? If so, when are data encrypted? Are data encrypted while at rest?Are data ever transported between locations across secured boundaries such as a secure data network (SDN), virtual private network, or Secure File Transfer Protocol (SFTP)? |
| Assess training needs | Do all programs involved have specific security and confidentiality training? How often is it conducted and who does it? What additional training will be required if policies are modified?Do other types of employees need to be trained (e.g. mail room staff, maintenance and cleaning staff, security staff, IT staff [in-house and contracted services])?How often are training materials updated?  |