**Data Security and Confidentiality Tool - 4**

**Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and
Use of Surveillance Data for Public Health Action**

**Frequently Asked Questions**

**1. Why are these not titled “Guidelines for Sharing Data”? Why don’t they have the word “sharing” in the title?**

These guidelines provide standards for security and confidentiality for data in all programs funded by the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP). Sharing is facilitated when the lack of protection is no longer a barrier for programs that conform to these guidelines. Data sharing standards are included as part of these guidelines, however, this document does not specify details of how, what, or when data should be shared.

**2. Do these replace the HIV Security and Confidentiality Guidelines?**

Yes. These replace the *Technical Guidance for HIV/AIDS Surveillance Programs, Volume III: Security and Confidentiality Guidelines* and establish formal security and confidentiality guidelines for HIV, viral hepatitis, STD, and TB programs funded through NCHHSTP.

**3. How do these fit with the Partner Services Security and Confidentiality Guidelines?**

These replace the data security and confidentiality guidelines contained in Appendix D, "Guiding Principles and Standards for Record Keeping and Data Collection, Management, and Security for Partner Services Programs for HIV Infection, Syphilis, Gonorrhea, and Chlamydial Infection" of the *Recommendations for Partner Services Programs for HIV Infection, Syphilis, Gonorrhea, and Chlamydial Infection*.

**4. Do these guidelines apply to CDC-funded prevention activities?**

Yes. All programs funded by NCHHSTP will be required to implement these guidelines for personally identifiable or potentially personally identifiable information. Beginning in 2012, adhering to the Guidelines is being incorporated into all core funding announcements. Surveillance programs, prevention programs, and programs who receive surveillance or program data are within the scope of these Guidelines.

**5. What are the minimum standards in this document? Should the document differentiate between the minimum and the ideal?**

The Guidelines are divided into five main topic areas and corresponding standards. All standards listed are required and every program must meet these. However, they are broadly stated to allow flexibility for implementation. Guiding questions, notes, and criteria are provided to assist programs in determining whether the standards are met.

**6. Will training materials be available to help programs implement the Guidelines?**

Yes. Training materials, webinars, toolkits, and other materials will be made available and posted on the PCSI Web site. The current Appendix contains information to support initial and periodic assessments.

<http://www.cdc.gov/nchhstp/programintegration/Default.htm>.

**7. Will CDC provide monitoring and/or technical assistance for programs implementing the Guidelines?**

Yes. Some technical assistance (TA) in monitoring and/or conducting initial assessments of data security and confidentiality protections may be available on a limited basis from NCHHSTP. Information regarding other potential resources will be made available by surveillance programs in each Division.

**8. Do employees working in viral hepatitis, STD, and TB programs need to have the same training for security and confidentiality as employees working in an HIV program?**

Yes. All health department staff in HIV, AIDS, viral hepatitis, STD, and TB programs with the same responsibilities and access to Personally Identifiable Information (PII) should have the same training. Other employees or contractors (custodial, security, etc.) may have more general security training. Areas may find it helpful to design training modules based on roles, responsibilities, and access to PII.

**9. Will CDC funding be available to support security and confidentiality activities, including physical environment changes?**

Yes. CDC is committed to assisting programs in meeting the Guidelines through TA and funding to the extent possible. In 2011–12, supplemental funding was made available through HIV Surveillance Funding Announcements. Additional financial support may be forthcoming through core prevention funding announcements from each Division. The new Guidelines will be referenced as a requirement of funding when new funding announcements are issued. Please work closely with your CDC Project Officers for your specific needs.

**10. To what extent are programs not funded by NCHHSTP required to implement these Guidelines?**

Programs that are not funded by NCHHSTP are not required to follow these Guidelines. Programs would only be required to implement these Guidelines if a funded program shared data with an unfunded program.

**11. When do the NCHHSTP Data Security and Confidentiality Guidelines go into effect?**

CDC expects these Guidelines to be part of all newly developed cooperative agreements and funding announcements. The Guidelines will go into effect when they are referenced and become a requirement in new funding announcements.

**12. What happens if we do not (or cannot afford to) implement these Guidelines across all of our programs?**

You should contact your CDC Project Officer as soon as possible to discuss any issues or barriers to implementation.

**13. If we have one set of guidelines in the department for all four programs, does that mean we have to all have the same set of standard operating procedures (SOPs)?**

No. Different programs may have different SOPs, all of which follow the same data security and confidentiality guidelines.

**14. If a program currently uses several Microsoft Access databases for data back-ups that do not meet the encryption standards listed in the Data Security and Confidentiality Guidelines, what will happen if these Guidelines are implemented?**

If these databases contain identifying, or potentially identifying information, they need to be modified, encrypted, or otherwise destroyed in accordance with locally developed policies.

**15. Do all programs have to share all of their surveillance data?**

No. Jurisdiction-specific decisions are based on local priorities, resources, need, etc. However, all NCHHSTP-funded programs are encouraged to utilize their data for public health action and to share data when appropriate to ensure public health and program effectiveness.

**16. How does this affect state health departments who work with local health departments and/or community-based organizations (CBOs)? Are these Guidelines intended to apply to sub-grantees as well as the state health departments?**

NCHHSTP-funded programs should work collaboratively with local health departments and other public health partners to ensure that data security and confidentiality policies and procedures exist in the other programs that conform to these Guidelines. State programs that subcontract directly with local health department programs may include compliance with these Guidelines in their contractual arrangements. Local health departments that share data with state health departments should take steps to share data using the secure methods outlined in this document. Local health departments can also hold annual trainings on these policies and procedures, and the NCHHSTP-funded programs can assist in these efforts both in establishing SOPs and trainings. NCHHSTP-funded programs may provide assistance to private providers and laboratories in implementing secure methods for reporting case data. Providers and laboratories should be encouraged to establish policies and procedures and hold regular trainings on data security and confidentiality.

**17. Who is responsible for the data provided by the program to the county and tribal levels?**

The overall responsible party (ORP) ensures the quality and safety of the data provided by the funded program to the county and tribal levels.

**18. Are local health departments expected to have ORPs even if they do not receive direct funding from CDC but receive funds from and/or work with their state health department?**

No. However, they are expected to have a point of contact for all matters concerning data security and confidentiality.

**19. Do the Guidelines apply to all contractors or just those with a contract for surveillance activities?**

All persons who have access to data from NCHHSTP-funded programs must abide by the principles and standards of the Guidelines.

**20. Do the Guidelines apply if an agency has a contract that is not surveillance-specific but has data that the department would interpret as being surveillance data—even if they did not collect it as surveillance data and would not define it as such?**

Yes. If the agency is collaborating with the health department on a project or effort involving surveillance data, they must maintain the same level of data security as the health department.

**21. Can a state apply these standards to all notifiable diseases if they wish to expand their use to non-NCHHSTP-funded programs?**

Yes. All public health programs could benefit from following consistent, documented security, and confidentiality guidelines for public health data.

**22. Do HIV, viral hepatitis, STD, and TB programs in an agency need to have a separate secure room for employees and to store this data?**

No. Each program does not necessarily need to have a separate secure room, but they do need to house data in a secure physical area with limited access. Some areas may have a secure section of a floor or an entire floor. The guidance for conducting an initial assessment for data security and confidentiality protections in the Guidelines may help you enhance your current space if needed. A checklist is also provided in the Appendix of the Guidelines.

**23. Why is it necessary to have a secure area? Can’t we assume that state and local health department offices are secure and that we can talk openly?**

It is necessary to have a secure area as outlined in the Guidelines for accessing or otherwise using PII. This includes areas for viewing data, discussing case information, counseling clients/patients and other work related activities. Assumptions cannot be made about the security of any location without an assessment. Most health department offices (state, county, or local) have some areas accessible to the general public, clients, or other non-employees. Conducting an initial assessment will assist staff with identifying possible risks to be mitigated.

**24. Do HIV, viral hepatitis, STD, and TB programs need to have a separate written policy for data security and confidentiality?**

No. It’s an agency-level decision whether to have one integrated document that covers all programs or individual policy documents for each program. All policies, however, should adhere to the NCHHSTP Data Security and Confidentiality Guidelines.

**25. Do the Guidelines apply to the use of surveillance or program data for research?**

Yes but there may be additional requirements. While the use of public health data for research may be permissible, IRB review is recommended and, in many instances, required. Questions regarding distinguishing research activities from practice are beyond the scope of these Guidelines and programs should be directed to applicable guidance related to the human subjects regulations and other guidance (e.g., the Council for State and Territorial Epidemiologists’ document on Public Health Practice vs. Research).

**26. Do the HIPAA requirements related to data access (e.g., logs, audits, etc.) apply to any data shared?**

No. Public health data used for surveillance and other public health uses are specifically excluded from HIPAA requirements for auditing access in individual medical records. For more information access Health and Human Services, Health Information Privacy web page
<http://www.hhs.gov/ocr/privacy/hipaa/faq/public_health_uses_and_disclosures/465.html>

**27. If the health department shares surveillance data with providers, does it then become a medical record subject to applicable laws?**

No. While there may be some clinical data contained in surveillance data shared with providers, surveillance data are not medical records and should not be treated as such.

**28. Is the medical provider able to access state surveillance records in making care decisions?**

In limited instances, yes. However, providers should utilize the most accurate and timely clinical information in making decisions and surveillance data are not typically the timeliest information available. Even laboratory results should be available directly from a laboratory more quickly than from a surveillance program.

**29. Are agency personnel required to shred documents to be destroyed or is it acceptable to use a third party document company?**

No. Agency personnel are not required to shred documents themselves—contracting with a document shredding service may be an option for some programs. If this is done, it is advisable to make arrangements to have the documents shredded on site or elsewhere with program staff present at least the first time the service used. In all cases, a contracted shredding or disposal company must be bonded and due diligence needs to be taken in their selection.

**30. Health departments often send faxes to a variety of different provider’s practices and hospitals. Completing case reports as faxes are a common way of reporting in some health departments. How can this be done without providing some PII? Are they now forbidden to use faxes?**

No. Use of fax machines for transmission of public health information containing PII is permitted, but discouraged. If you must send a fax, specific guidance is provided on ways you can minimize risk in Appendix F of the Guidelines.

**31. In many states, viral hepatitis and TB data are housed in National Electronic Disease Surveillance System (NEDSS), or NEDSS-like, applications. In general, NEDSS applications are networked and many are also Internet-based applications. How do we ensure these applications meet standards for IT practices included in the Guidelines?**

Conducting an initial assessment would help ensure that these applications meet standards for IT practices included in the Guidelines. The initial assessment process includes other systems and documents users, access, roles, rights, availability, etc. in these NEDSS or NEDSS-like applications in the same manner it would assess any other system.

**32. The state electronic disease reporting system allows local administrators to decide who has access to the system and their security roles for certain disease groups. Would this be allowed under these Guidelines?**

Yes. State and local SOPs would still be in place for specific systems. CDC would expect role-based access to continue to be in place and for the administrators to follow these Guidelines.

**33. Do these Guidelines suggest that Web-based surveillance systems are not secure?**

No. Web-based surveillance systems cannot all be classified as fully secure or not secure. These systems, as with other data sources and/or data repositories, must be looked at on an individual basis. These systems should undergo assessments to ensure they meet the security standards. This should include review of access, roles, rights, procedures, etc., similar to other systems. For instance, access from a provider’s office or lab for reporting may be secured through various means (VPN, digital certificates, etc.), as can access by a field worker checking on potential new reports or updates. However, access from a coffee shop, fast-food establishment, or other Wi-Fi hotspot must be prevented.

**34. More and more systems are using advanced technologies which are not mentioned in the Guidelines. What about future technologies?**

Predicting technology advancements in the present time is impossible. Any new technology or advancement must be examined with due diligence, weighing benefits and mitigating risks. It would be advantageous to establish a policy for implementing new technologies that includes some type of requirements for program review and approval, in addition to any IT review and approval.

**35. As more and more areas institute telework as an option, can surveillance data be accessed remotely?**

Yes. With appropriate precautions, policies, and training in place, remote access is possible. Appendix G of the Guidelines contains requirements to be met in a telework environment, as well as other remote work locations.