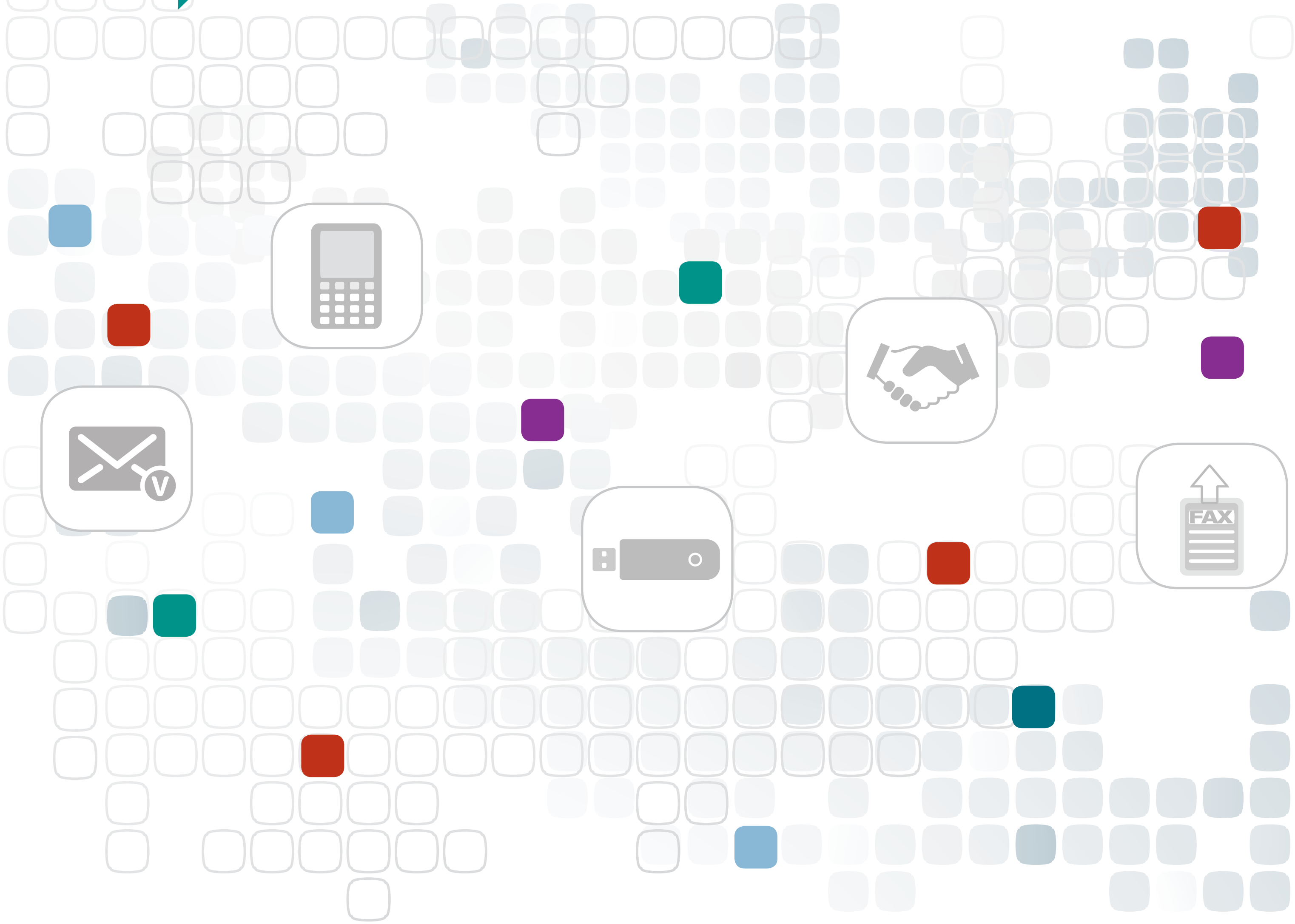
Data Security and Confidentiality Guidelines

for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs:

Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action



National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention

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

Suggested Citation: Centers for Disease Control and Prevention. 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.
Atlanta (GA): U.S. Department of Health and Human Services, Centers for Disease Control and Prevention; 2011

This report was prepared by

Security and Confidentiality Guidelines Subgroup of CDC's NCHHSTP Surveillance Work Group:

Patricia Sweeney, Sam Costa;
Division of HIV/AIDS Prevention

Hillard Weinstock , Patrick Harris, Nicholas Gaffga;
Division of STD Prevention

Kashif Iqbal;
Division of Viral Hepatitis

Lilia Manangan, Suzanne Marks;
Division of TB Elimination

Gustavo Aquino;
Office of the Director, NCHHSTP

This publication lists non-federal resources in order to provide additional information to consumers. The views and content in these resources have not been formally approved by the U.S. Department of Health and Human Services (HHS). Listing these resources is not an endorsement by HHS or its components.

Table of Contents

I. Executive Summary

A goal of CDC's National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP) is to strengthen collaborative work across disease areas and integrate services that are provided by state and local programs* for prevention of HIV/AIDS, viral hepatitis, other sexually transmitted diseases (STDs), and tuberculosis (TB). A major barrier to achieving this goal is the lack of standardized data security and confidentiality procedures, which has often been cited as an obstacle for programs seeking to maximize use of data for public health action and provide integrated and comprehensive services.

Maintaining confidentiality and security of public health data is a priority across all public health programs. However, policies vary and although disease-specific standards exist for CDC-funded HIV programs, similarly comprehensive CDC standards are lacking for viral hepatitis, STD, and TB prevention programs. Successful implementation of common data protections in state and local health departments with integrated programs suggest implementation of common data security and confidentiality policies is both reasonable and feasible. These programs have benefited from enhanced successful collaborations citing increased completeness of key data elements, collaborative analyses, and gains in program efficiencies as important benefits. Despite the potential benefits, however, policies have not been consistently implemented and the absence of common standards is frequently cited as impeding data sharing and use. Adoption of common practices for securing and protecting data will provide a critical foundation and be increasingly important for ensuring the appropriate sharing and use of data as programs begin to modify policies and increasingly use data for public health action.

This document recommends standards for all NCHHSTP programs that, when adopted, will facilitate the secure collection, storage, and use of data while maintaining confidentiality. Designed to support the most desirable practices for enabling secure use of surveillance data for public health action and ensuring implementation of comprehensive evidence-based prevention services, the standards are based on 10 guiding principles that provide the foundation for the collection, storage, and use of these public health data. They address five areas: program policies and responsibilities, data collection and use, data sharing and release, physical security, and electronic data security. Intended for use by state and local health department disease programs to inform the development of policies and procedures, the standards are intentionally broad to allow for differences in public health activities and response across disease programs.

The standards, and the guiding principles from which they are derived, are meant to serve as the foundation for more detailed policy development by programs and as a basis for determining if and where improvements are needed. The process includes seven main steps: designating an overall responsible party; performing a standards-based initial assessment of data security and confidentiality protections; developing and maintaining written data security policies and procedures based on assessment findings; developing and implementing training; developing data-sharing plans or agreements as needed; certification of adherence to standards; and

*State and local is inclusive of state, tribal, local and territorial health departments and agencies.

performing periodic reviews of policies and procedures. NCHHSTP-funded programs will also be required to verify their adherence to the standards through submission of certification statements. CDC will work with state and local health departments to monitor the implementation of the guidelines and evaluate their impact on securing data, facilitating data use, and increasing program effectiveness.

This document reflects the combined efforts of NCHHSTP's Surveillance Workgroup members, composed of surveillance leaders from NCHHSTP's Division of HIV/AIDS Prevention (DHAP), Division of Viral Hepatitis (DVH), Division of STD Prevention (DSTDP), and Division of TB Elimination (DTBE). The work was informed by consultation with state and local public health leaders and public health organizations representing HIV, viral hepatitis, STD and TB disease disciplines (see Acknowledgements section). The document supersedes previously published security and confidentiality guidelines for HIV surveillance and establishes data security and confidentiality standards for viral hepatitis, STD, and TB. Establishment of these standards that apply to all surveillance activities in all of the Center's divisions will facilitate collaboration and service integration among NCHHSTP-funded programs with minimal risk of inappropriate release of confidential, identifiable surveillance data or misuse of those data in pursuit of legitimate public health purposes.

II. Introduction

The true value of surveillance is measured by its impact on public health action and practice.[1] Public health agencies at all levels have broad authority to collect, store, and use personal health information to identify, report, and control health threats and to plan, implement, and evaluate public health programs and services. The public trusts that any personal or confidential information collected as part of public health activities will be held securely and confidentially and will be used for legitimate public health purposes. Although protections exist through various laws, policies and procedures, these protections vary across jurisdictions[2-4] and sometimes even within public health organizations.[5]

A goal of CDC's National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP) is to strengthen collaborative work across disease areas and integrate services that are provided by programs for prevention of HIV/AIDS, viral hepatitis, other sexually transmitted diseases (STDs), and tuberculosis (TB).[6] A major barrier to achieving this goal is the lack of standardized data security and confidentiality procedures, which has often been cited as an obstacle for programs seeking to maximize use of data for public health action and provide integrated and comprehensive services.[7] Although disease-specific standards exist for CDC-funded HIV programs,[8,9] similarly comprehensive CDC standards are lacking for viral hepatitis, STD, and TB prevention programs.

CDC established data security and confidentiality guidelines for CDC-funded HIV surveillance programs in state and local* health departments in 1998[8] and updated the guidelines in 2006.[9] The guidelines emphasize the protection of surveillance data and prohibit HIV surveillance programs from sharing data with programs that lack equivalent data security and confidentiality protections. These restrictions on data sharing had the unintended consequence of inhibiting the ability of some local health departments to link clients to appropriate treatment and prevention services.[7,10]

In 2008, CDC published updated recommendations for programs providing partner services for HIV, syphilis, gonorrhea, and chlamydial infections. The document includes recommendations related to record keeping, data collection, data management, and data security that were based on previously published HIV surveillance guidelines.[11] The partner services recommendations encourage data linkage and sharing between public health service-provision prevention programs and disease-reporting surveillance systems. The recommendations suggest that sharing of individual-level surveillance data can help facilitate the timely provision of partner services but also underscore the need for well-defined security and confidentiality policies and procedures. Despite the potential benefits, however, these have not been consistently implemented.

In addition, CDC cooperative agreements with TB programs require that policies and procedures must be in place to protect the confidentiality of all TB surveillance case reports and files. TB programs should also collaborate with HIV/AIDS programs to conduct at least annual TB and AIDS registry matches to ensure completeness of reporting of HIV and TB coinfected patients to both surveillance systems. However, this collaboration has been hampered by perceived differences in policies and procedures to protect HIV test results.

This document does not specify details of how, what or when data should be shared but rather establishes standards of data protection across programs that should be in place. Intended for use by state and local health department disease programs to inform the development of policies and procedures, the standards are intentionally broad to allow for necessary differences in public health activities and response across disease programs. The extent to which data are used for public health interventions and follow-up with individuals, and to which health department programs interact or share data with reporting physicians and health providers, will vary according to established program practices.

This document reflects the combined efforts of NCHHSTP's Surveillance Workgroup members, composed of surveillance leaders from NCHHSTP's Division of HIV/AIDS Prevention (DHAP), Division of Viral Hepatitis (DVH), Division of STD Prevention (DSTDP), and Division of TB Elimination (DTBE). The document supersedes previously published guidelines for HIV surveillance and partner services and establishes up-to-date data security and confidentiality standards of viral hepatitis, STD, and TB.

*State and local is inclusive of state, tribal, local and territorial health departments and agencies.

Key Definitions Used in this Document

Data sharing: Granting certain individuals or organizations access to data that contain personally identifiable information with the understanding that personally identifiable or potentially identifiable data cannot be re-released further unless a special data-sharing agreement governs the use and re-release of the data and is agreed upon by the receiving program and the data provider(s).

Data-sharing agreement: Mechanism by which a data requestor and data provider can define the terms of data access that can be granted to requestors.

Data release: Dissemination of data either in a public-use file or as a result of an ad hoc request which results in the data steward no longer controlling the use of the data. Data may be released in a variety of formats including, but not limited to, tables, microdata (person records), or online query systems.

Data dissemination: Any mechanism by which data are made available to users. Includes mechanisms whereby data are released to users as well as mechanisms whereby data are made available without being released.

Personally identifiable information: As defined by National Institute of Standards and Technology Special Publication 800-34, Guide To Protecting The Confidentiality of Personally Identifiable Information: "Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. "[12]

Adapted from: CDC/ATSDR data release guidelines and procedures for re-release of state-provided data.[4] See glossary in Appendix A for additional definitions of terms used in this document.

III. About this Document

This document recommends standards for data security, confidentiality, and use across surveillance and program areas for HIV, viral hepatitis, STD, and TB prevention in state and local health jurisdictions. The standards support the most desirable practices for enabling secure use of data and ensuring comprehensive preventive services while being broad enough to allow for differences in public health activities by disease program. The standards address five areas: program policies and responsibilities, data collection and use, data sharing and release, physical security, and electronic data security.

The standards are based on 10 guiding principles that provide the foundation for the collection, storage, and use of surveillance data for public health action. The guiding principles are derived from existing CDC policies and guidelines, model and existing legislation, and from related work, including current security and confidentiality principles for NCHHSTP's HIV surveillance programs and practical application of ethics in public health surveillance.[8,9,11,13-20] Similar principles have been proposed as part of a national strategy[21] consistent with public health values[22,23] to ensure the privacy and security of public health data at all levels.

The standards are intended to apply to public health programs funded by NCHHSTP (including those of state and local health departments and their contractors) that are responsible for collecting, storing, and using surveillance data and to any entities with which these programs share data. The standards address the use of both identifiable (i.e., personally identifiable information [PII]) and nonidentifiable data and may include: data used for epidemiologic investigations; data used to link patients with partner services, appropriate treatment, interventions, and other health services; and data used for case management and program evaluation. Because the use of identifiable data requires a higher level of protection than the use of nonidentifiable data, the document includes specific standards for the sharing of identifiable data. Key definitions for data sharing, data release, data release agreement, data dissemination, and personally identifiable information are highlighted in the box above and additional terms are provided in the Glossary (Appendix A).

IV. Using this Document

Active data stewardship involves developing proactive policies, procedures, and training to ensure that public health data are collected, stored, and used appropriately. To that end, policies related to the security and sharing of data should be reviewed regularly and changed as needed. The data standards and the guiding principles from which they are derived are meant to serve as the foundation for more detailed policy development by programs and as a basis for determining if and where improvements are needed. Key components of data security and confidentiality, sharing, and use policy development are outlined below.

Overall Responsible Party (ORP)—A high-ranking official should be identified to accept overall responsibility for implementing and enforcing data security, confidentiality and sharing standards. This official should have the authority to make decisions about program operations that might affect programs authorizing, accessing or using the data, and should serve as the contact for public health professionals regarding security and confidentiality policies and practices. If the required span of control is not under a single person's purview, several persons can serve in the capacity of ORP as an ORP panel.

Initial Assessment of Data Security and Confidentiality Protections—This document is intended to serve as a planning resource for use by state and local public health programs to develop or upgrade their data security and confidentiality policies and procedures. An initial assessment will be particularly useful for state and local public health programs that currently lack data security and confidentiality policies and procedures.

A team led by the ORP should conduct an initial assessment of current data security and confidentiality protections. The team should include:

- Program managers, directors, or equivalent leaders from participating programs
- Other representatives of participating programs who may provide insight on access requirements and procedures for certain jobs or duties (e.g., surveillance staff, DIS data managers)
- Staff members with technical expertise in data security

Information technology (IT) staff should be involved at an early stage to ensure that they understand the data security and confidentiality standards and are fully engaged in the overall process. This involvement is critical as areas move to more centralized IT services and, in some cases, outsourced IT services.

The initial assessment should include the following steps:

- Identify key individuals and designate an ORP or ORP panel
- Review current security and confidentiality-related materials (e.g., written policies, procedures)
- Review relevant state and local laws that might affect data security and confidentiality policies
- Identify any policies or procedures that are either sources of data security weaknesses or barriers to information sharing and 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 electronic data transfer and storage
- Assess factors related to security of information in the field
- Assess training needs

Sample checklists for conducting initial and comprehensive assessments are provided in Appendix B.

Data Security and Confidentiality Policies and Procedures—Programs required by NCHHSTP to meet these guidelines are responsible for developing and maintaining written, program-specific data security and confidentiality policies and standard operating procedures, based on these guidelines, the assessment findings and in the context of state and local laws. Legislative and regulatory barriers to these standards should be addressed. State health department programs should work collaboratively with local health departments and public health partners involved in surveillance and prevention-related activities to maintain equivalent standards to the extent possible. 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 share data using the secure methods outlined in this document. 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 regular training on data security and confidentiality, according to these standards.

When public health data are collected or used as part of federally funded research, they are also subject to the federal policy for the protection of human subjects as described in the Code of Federal Regulations, Title 45, Part 46.[24]

Training—Staff members authorized to access and use public health data are responsible for adhering to their programs' data security and confidentiality policies and procedures and should receive ongoing training on an annual basis on the appropriate collection, storage, use, and dissemination of data as defined by these policies.

Data-Sharing Plans—Shared data facilitates identification of populations at risk for multiple infections and the design and implementation of programs that comprehensively address identified needs. A written plan can serve as a starting point for discussions about data sharing between or among public health programs. A data-sharing plan should include:

- Intent and scope of data sharing
- Potential benefits (including projected efficiencies) and risks of sharing, benefits and risks of not sharing, and methods to monitor these benefits and risks
- Methods that will be used to share data and roles and responsibilities of staff involved
- Minimum data elements needed to achieve the objective(s), including need for PII
- Steps that will be taken to ensure the confidentiality and security of shared data
- Provisions for physical and electronic security
- How shared data will be used, analyzed, published, released, and retained/destroyed
- Confidentiality agreements
- Knowledge and training requirements including annual training for staff who have access to PII and non-PII data

Although a written plan might not seem necessary between programs in the same health department or in integrated programs, having a plan in writing can help in resolving any conflicts. A more formal agreement, such as a data-sharing agreement or Memorandum of Understanding (MOU) may be required in certain circumstances (e.g., sharing outside the health department or with another public health organization). Programs can consult legal experts in their organizations to determine the need for a formal agreement.

Appendix C includes an example of one method of data sharing to improve program efficiencies and effectiveness.

Certification—Programs are required to self-certify their adherence to the standards for ensuring the security, confidentiality, and appropriate use of the data they collect, store, and share. The certification statement should:

- Identify one or more persons as the ORP for ensuring adherence to the standards
- Attest to adherence to all standards, or explain any lapses
- If lapses, describe steps to meet the standards in the future
- Describe policies and procedures instituted to ensure continued adherence to the standards

NCHHSTP will describe the certification process in applicable program announcements. NCHHSTP will conduct periodic reviews of the data security, confidentiality and sharing procedures of grant recipients during routine site visits and provide technical assistance as needed.

A suggested format for a certification statement is provided in Appendix D.

Periodic and Ongoing Reviews and Assessments—Programs should review their data security, confidentiality, and sharing policies and procedures at least annually or sooner if improved technologies or legislative/regulatory changes occur and revise as necessary. In addition, they should periodically assess whether other changes in personnel, programs, organizations, or priorities require changes in policies and procedures. For example, changes in federal standards for encryption could affect existing policies and procedures and require software updates or other revisions.

Programs should also review their data-sharing plans or agreements periodically in light of improved technologies and revise as necessary. Tracking the security and confidentiality training of staff members authorized to access data, including documenting and storing their signed confidentiality agreements, should also be part of ongoing assessment activities.

V. Benefits, Risks, and Costs of Sharing Data and Maintaining Security and Confidentiality

There is a balance that must be maintained between protecting the individual and the public from disease and protecting individuals' confidentiality and right to privacy. Both are vital to enhancing the public's health and maintaining the public's trust. Programs that have and follow consistent guidelines for the collection, storage, and use of HIV, viral hepatitis, STD, and TB data may reassure individuals, and the public, that sharing data for public health action will not compromise confidentiality.

Adherence to harmonized standards for data security across programs will enhance the ability to share data without compromising confidentiality. As programs consider how best to meet these standards, it is helpful to consider the benefits, risks, and costs. The public health benefits of sharing data among HIV, viral hepatitis, STD, and TB programs include the following:

- Early case detection and accurate and timely reporting of diseases
- Improved efficiencies in use of human and financial resources to achieve program objectives
- Improved projections of human and financial resources for disease programs and specific projects
- Improved opportunities to inform providers and patients about standards of care and needs for additional care
- Enhanced quality of surveillance data across programs
- Improved documentation and reporting of co-morbidities, leading to better patient management and partner services
- Better understanding of patients' health status to ensure comprehensive care and avoid redundant services and missed opportunities for prevention
- Increased understanding of how epidemics interact synergistically (syndemics), geographically, within population subgroups, or within groups engaging in specified high-risk behaviors
- Identification of specific populations that need outreach with consistent messages and targeted testing and service provision

Although data sharing has many benefits, there are also some risks. Despite the public health community's excellent track record in managing sensitive data, security breaches can occur. Harmonized data security and confidentiality standards among programs, and a commitment to enforcing them, can, however, minimize these risks. Breaches involving electronic data with identifiable information (e.g., human error resulting in reports going to the wrong patient or provider or databases being stolen or accessed illegally) might cause greater harm because more information about more individuals is released. Therefore, procedures for electronic data security must be developed. However, there are also some risks to not sharing data. Individuals might not receive prevention services, clients might not receive appropriate treatment, clients might not receive treatment at all, and disease transmission might increase.

Costs associated with improvements in data security can be a barrier to data sharing. To facilitate data sharing, hardware and software systems need to be compatible. Electronic transfer of data needs to be performed securely. Storage of data needs to be secure and remain confidential at all levels. Additional computer programming support may be required to facilitate secure data sharing across programs, conduct data matches, meet systems requirements, and de-duplicate data.

VI. Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality

The 10 principles below are intended to guide NCHHSTP-funded programs in developing data security and confidentiality policies. The principles should guide the collection, storage, and use of data for legitimate public health purposes. Legitimate public health purposes can be defined as a population-based activity or individual effort aimed primarily at the prevention of injury, disease, or premature mortality. This term also refers to the promotion of health in the community, including 1) assessing the health needs and status of the community through public health surveillance and epidemiologic research; 2) developing public health policy; and 3) responding to public health needs and emergencies. Public health purposes can include analysis and evaluation of conditions of public health importance and evaluation of public health programs. The principles also underpin the data security standards defined in the following section.

TEN GUIDING PRINCIPLES FOR DATA COLLECTION, STORAGE, SHARING, AND USE TO ENSURE SECURITY AND CONFIDENTIALITY

1. Public health data should be acquired, used, disclosed, and stored for legitimate public health purposes.
2. Programs should collect the minimum amount of personally identifiable information necessary to conduct public health activities.
3. Programs should have strong policies to protect the privacy and security of personally identifiable data.
4. Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.
5. Programs should have policies and procedures to ensure the quality of any data they collect or use.
6. Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.
7. Programs should share data for legitimate public health purposes and may establish data-use agreements to facilitate sharing data in a timely manner.
8. Public health data should be maintained in a secure environment and transmitted through secure methods.
9. Minimize the number of persons and entities granted access to identifiable data.
10. Program officials should be active, responsible stewards of public health data.

Adapted from: Lee, LM, Gostin, LO. Ethical collection, storage, and use of public health data: a proposal for national privacy protection. JAMA 2009;302:82–84