Maryland Department of Health and Mental Hygiene

Prevention and Health Promotion Administration

Infectious Disease Bureau

Data Security and Confidentiality Guidance

for

Infectious Disease Programs

September 5, 2013

TABLE OF CONTENTS

Introduction

Rationale

The Maryland Department of Health and Mental Hygiene, Prevention and Health Promotion Administration, Infectious Disease Bureau is charged with collecting, storing, and using personally identifiable information (PII) to identify and control infectious diseases and other public health conditions and to evaluate public health programs and services for the state of Maryland. The public trusts that any personal or sensitive information collected as part of public health activities will be held securely and confidentially and will only be used for legitimate public health purposes. Release of directly or indirectly personally identifiable information, whether intentionally or unintentionally, could result in negative consequences, both for individuals about whom data are collected and for the programs that collect and use this information. Some possible negative consequences for individuals may include decline in property value, loss of employment, legal prosecution, personal embarrassment, loss of health care, and threats of physical violence. Negative consequences for programs may include decreased ability to collect data, loss of public confidence and participation in the program, decreased provider cooperation, decreased ability to benefit the public, and threats of physical violence for service providers. The legal authority and requirements related to specific infectious disease programs are explained in each program's respective Procedures Manual.

The CDC's National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP) has prioritized program collaboration and service integration (PCSI). It is working to strengthen collaborative work across disease areas and integrate client-level services that are provided by related programs, especially care and prevention activities related to HIV/AIDS, viral hepatitis, other sexually transmitted diseases (STDs), and tuberculosis (TB). PCSI is a mechanism for organizing and blending interrelated health issues, activities, and prevention strategies to facilitate a comprehensive delivery of services.[1]

Harmonizing confidentiality standards for the use of data in infectious disease programs will facilitate sharing of data for public health action, expand the use of surveillance information for care and prevention programs, improve our understanding of the "syndemic" relationship of infectious diseases—how they interact synergistically to produce an excess burden of related diseases in specific populations, and help enhance the quality of data across programs. This understanding is a necessary step toward supporting CDC's PCSI goals. Current policies and standards for securing and managing personally identifiable information in infectious disease programs vary, and

[1] Centers for Disease Control and Prevention. Program Collaboration and Service Integration: Enhancing the Prevention and Control of HIV/AIDS, Viral Hepatitis, Sexually Transmitted Diseases, and Tuberculosis in the United States. Atlanta (GA): U.S. Department of Health and Human Services, Centers for Disease Control and Prevention; 2009.

the lack of standardization has often been cited as a critical barrier to sharing data across programs. Broad adherence to standardized data security policies across programs would enhance the programs' abilities to share important health data, enhance data quality, and potentially improve the provision of public health services. It would also reduce the risk that public health data are used inappropriately without becoming a barrier to program effectiveness.[2]

The data security rationale and standards outlined in this document are based on: 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. These CDC Guidelines are required for all CDC funded HIV, viral hepatitis, sexually transmitted disease, and tuberculosis surveillance programs and for the programs with which they share data.

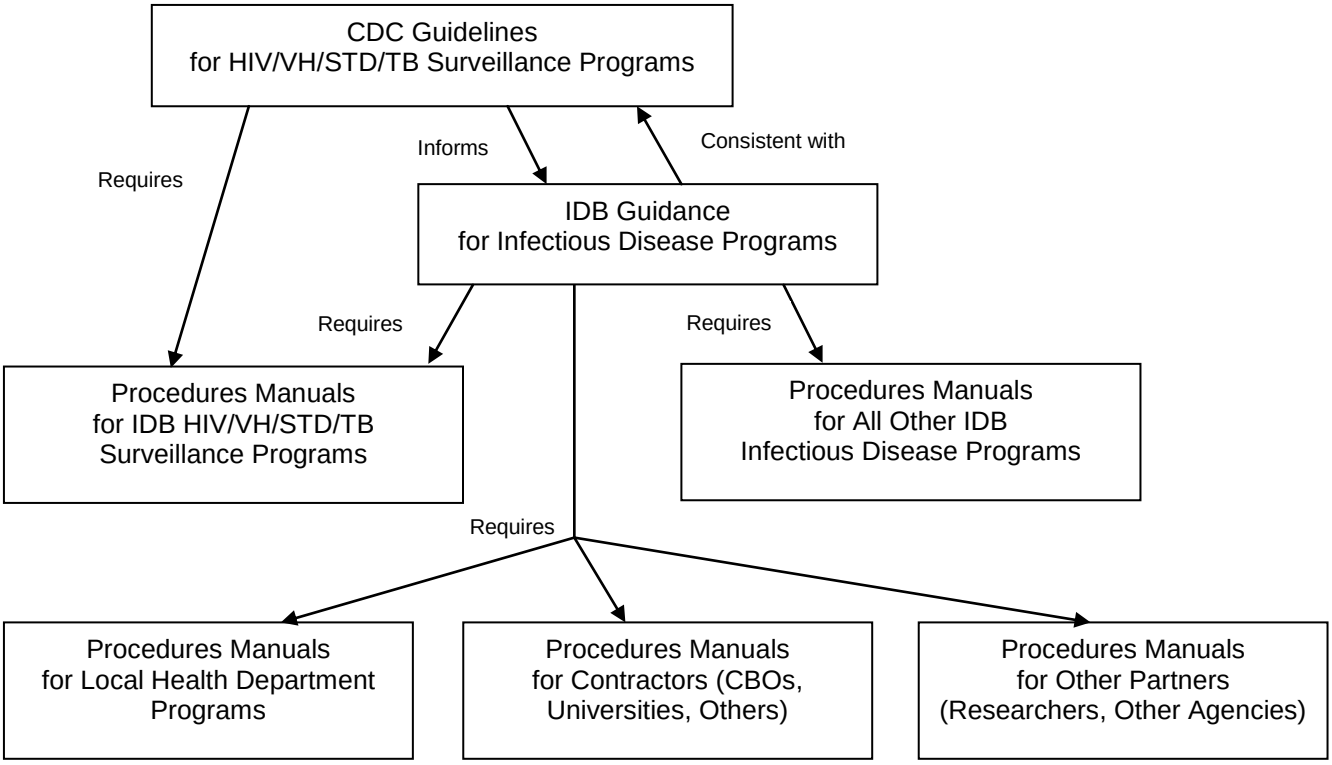
This Maryland Department of Health and Mental Hygiene, Prevention and Health Promotion Administration, Infectious Disease Bureau Data Security and Confidentiality Guidance (IDB Guidance) is consistent with the CDC Guidelines and defines confidentiality and data security standards for the collection, storage, sharing, and use of data across the surveillance, prevention, and care program areas of the Infectious Disease Bureau for the state of Maryland. The IDB Guidance applies to all state and local public health programs that collect or use personally identifiable information for the diseases under IDB that receive federal funding either directly or indirectly; to contractors responsible for collecting, storing, and using these programs' data; to any programs or other entities with which these programs may share data; and to information technology and other support staff that have access to the systems and facilities that house the data. This includes the specific Centers and Offices in IDB listed below and the programs which they manage. It also includes staff from the DHMH Office of Information Technology that provide technical support to IDB programs. Other PHPA Centers and Offices and their disease programs may also be covered by these IDB Guidelines at the discretion of the PHPA Director.

Infectious Disease Bureau Office of the Director (ODR)
- Office of Faith Based and Community Initiatives (OFBCI)
- Office of Immigrant Health (OIH)
- Office of Infectious Disease Epidemiology and Outbreak Response (OIDEOR)
  - Center for HIV Surveillance, Epidemiology and Evaluation (CHSEE)
  - Center for Immunization (CI)

[2] 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.

Center for Surveillance, Infection Prevention, and Outbreak Response (CSIPOR)
Center for Zoonotic and Vector Borne Diseases (CZVBD)
Emerging Infections Program (EIP)
Office of Infectious Disease Prevention and Care Services (OIDPCS)
Center for HIV Prevention and Health Services (CHPHS)
Center for Planning and Quality Improvement (CPQI)
Center for Sexually Transmitted Infection Prevention (CSTIP)
Center for Tuberculosis Control and Prevention (CTBCP)

Security and Confidentiality Framework



Each program is responsible for developing a program-specific Procedures Manual that describes the program's procedures for implementing data security and confidentiality in a manner consistent with the CDC Guidelines and this IDB Guidance. A program may be defined in several different ways, including 1) as all of the operations of an IDB Center, Office, or partner; or 2) as the operations related to a specific disease activity either within an IDB Center, Office, or partner or across multiple Centers or Offices.

For example, the tuberculosis surveillance, prevention, and care activities at the state-level may all occur in and be covered by the Data Security and Confidentiality Procedures Manual of the Center for Tuberculosis Control and Prevention.

In a second example, one county health department may decide to cover all of its infectious disease programs in one county-wide procedures manual, while another county may decide that it needs separate procedures manuals for its HIV program, its STI program, and its general communicable disease program.

For CDC-funded surveillance programs, the CDC is developing a review and certification process that reportedly will require each funded program to perform a self-assessment of their security and confidentiality procedures, prepare or update a set of written procedures, self-certify to the CDC that they meet the CDC Guidelines, and then submit their procedures for CDC review.

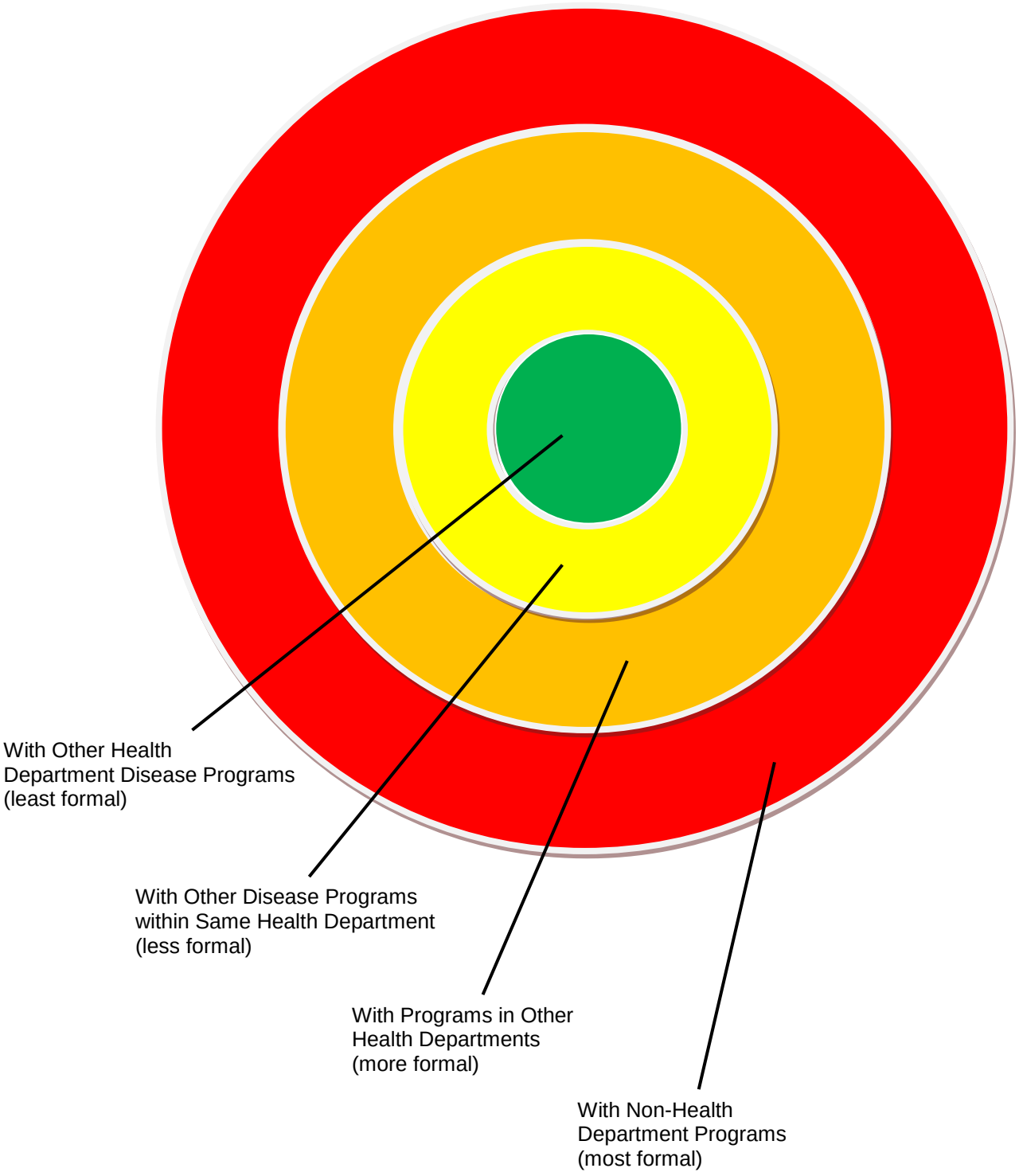
In 2012, all state IDB programs and local health departments completed a self-assessment and were instructed to begin to prepare their written procedures. This IDB Guidance requires all programs to complete the process of preparing written Procedures Manuals, to submit them to the IDB Director for inclusion as appendices to the IDB Guidance, and to self-certify that their Procedures Manual meets the requirements of the CDC Guidelines and the IDB Guidance.

Because one of the primary purposes of developing these data security and confidentiality procedures is to support data sharing, all programs should identify situations where their data are shared between programs and begin to develop Data Sharing Agreements. The need for a Data Sharing Agreement and the level of formality of the agreement will be dependent on the distance between the programs. For example, sharing data between two activities within a program should be covered in the program's Procedures Manual; sharing between two programs within the same health department should be covered in each programs' Procedures Manuals and there should be a signed agreement between the two program directors; whereas sharing between two different health departments will probably require a formal written agreement signed by appropriate agency heads; and sharing with a non-health department program may require a formal contract or legally-binding agreement.

Developing a Data Sharing Agreement should include a review of the appropriateness of the data sharing, an assessment of whether only the minimum amount of data necessary to accomplish the activity will be shared, and a review of the procedures for maintaining data security and confidentiality of the program receiving the shared data.

Data Sharing Agreements

The need for Data Sharing Agreements and their level of formality will depend on the distance between the programs sharing data.



The data security and confidentiality policies outlined in this IDB Guidance follow the five broad areas of data protection from the CDC Guidelines. They are:

1.0 Program policies and responsibilities;

2.0 Data collection and use;

3.0 Data sharing and release;

4.0 Physical security; and

5.0 Electronic data security.

Each of the five areas is broken down into specific standards set by the CDC Guidelines. Each standard is followed by a description of the measures to be taken by programs to meet the standard. Please note that the IDB Guidance includes standards that apply broadly across all IDB programs. Many of the standards call for program-specific procedures, and the appendices following this document contain the program-specific Procedures Manuals.

The IDB Guidance is intended to set minimum standards for infectious disease programs to permit and encourage data sharing between programs for public health action. The specifics of data sharing between programs are detailed in Data Sharing Agreements that are written by the programs and included in their Procedures Manuals.

Guiding Principles

The Centers for Disease Control and Prevention's (CDC's) National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP) has established 10 guiding principles for NCHHSTP-funded programs to use as a guide in developing their data security and confidentiality policies (CDC Guidelines, Section VII, p. 11).

These guiding principles from the CDC Guidelines also serve as a basis for the more detailed data security and confidentiality standards and underlie the policies in this IDB Guidance and the procedures in the program-specific Procedures Manuals.

TEN GUIDING PRINCIPLES FOR THE 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.	Program 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 aggregate/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.	A minimum number of people and entities should be granted access to identifiable data.
10.	Program officials should be active, responsible stewards of public health data.

Standards

The following standards were adopted from the standards set forth in the CDC Guidelines. Each standard begins with a listing of the individual standard contained in the CDC Guidelines; for example, **STANDARD 1.1** refers to the first requirement in the first section in the CDC Guidelines.

Each standard is followed by additional text that attempts to explain, clarify, or give examples of how to apply the standard. Some of these explanations may not apply to all programs, particularly to non-IDB programs. At the end of the additional text is a box that contains a summary of instructions for what should be included in the program-specific Procedures Manual for this standard. It is up to each program to determine which parts of each standard apply to their program and to describe their program's response in their Procedures Manual. Each program will self-certify that their procedures fulfill the requirements of the standards.

1.0: Program Policies and Responsibilities

STANDARD 1.1 – Develop written policies and procedures on data security and confidentiality; review all data policies and procedures at least annually; revise them as needed; and ensure their review by and accessibility to all staff members having authorized access to personally identifiable information.

This IDB Guidance and its appendices (program-specific Procedures Manuals) serves as the Maryland Department of Health and Mental Hygiene's written policies and procedures on infectious disease program data security and confidentiality. It applies to all infectious disease public health programs within the state administered by the Infectious Disease Bureau. The program-specific Procedures Manuals will provide details for each program, including state-level disease programs, local health department programs, and partners and contractors of the state and local health department programs.

Each program's Procedures Manual should include:

- Reviews of applicable laws and regulations
- Descriptions of applicable data (include details on types of records, systems, and reports)
- Roles and responsibilities of persons with authorized access to the data
- Applicable confidentiality pledges
- Controls for data management, security, and access (physical and electronic)
- Discussions of when use of privacy advice or reminder is appropriate (i.e., when to include privacy advice at the point of information use on forms, information

collection devices, systems, file cabinets, etc.)
- Specific procedures applicable to trainees, students, volunteers, visitors, and IT, cleaning, maintenance, and security staff
- Provisions to limit disclosure and prevent indirect release of personally identifiable information
- Procedures for data sharing

Each staff member with access to personally identifiable information should receive an orientation to security and confidentiality immediately upon starting work and sign a confidentiality pledge agreeing to adhere to all the policies and procedures. They should be made aware of the consequences if the pledge is not adhered to. Staff should be required to sign and renew their confidentiality pledge on an annual basis. There is a general IDB confidentiality pledge (Appendix A) and individual disease programs may have their own confidentiality pledges, which would then be described in the program's Procedures Manual.

Each program should review and evaluate their Procedures Manual at least annually. The Overall Responsible Party (ORP) Panel (see Standard 1.2) should review and evaluate the IDB Guidance at least annually. Results of these reviews and evaluations will be discussed with relevant staff, and staff members should be notified of any changes or updates to policies and procedures as they arise.

Security and confidentiality policies and procedures should be located in a place to which all staff have access.

The CDC Guidelines are available online at:
http://www.cdc.gov/hiv/resources/guidelines/security_confidentiality_hiv.htm

This IDB Guidance, including the appendices of program-specific Procedures Manuals. is available on the DHMH network at: [s-drive location]

Individual programs' Procedures Manuals should be made available to program staff.

Standard 1.1 Summary: Each program must develop a written program-specific Procedures Manual in accordance with the CDC Guidelines and the IDB Guidance and describe where copies of the Procedures Manual are located.

STANDARD 1.2 – Designate a person or persons to act as the overall responsible party (ORP) for the security of public health data your program collects or maintains, and ensure that the ORP is named in any policy documents related to data security.

Each program should designate its own ORP. Each ORP should be an official who has the authority to modify the program's data security and confidentiality procedures to ensure that standards are met.

Together the individual ORPs from the state-level IDB programs shall make up an IDB ORP Panel that should meet annually, or more frequently as needed. The IDB ORP Panel should review the IDB Guidance and recommend changes to the IDB Director. The IDB ORP Panel includes the ORPs designated within the following infectious disease programs:

- HIV health services
- HIV prevention
- HIV surveillance
- STI prevention
- TB control
- [LIST ALL DISEASE PROGRAMS WITH INDIVIDUAL PROCEDURES MANUALS – These are to be identified by the programs]

Standard 1.2 Summary: Each program should identify, in its Procedures Manual, the ORP by name and title and describe his/her role within the program.

STANDARD 1.3 – Ensure that data security policies define the roles and access level(s) for everyone with authorized access to personally identifiable information and the procedures for accessing data securely.

Staff with authorized access to public health data includes:

- Program staff who use the data daily.
- Staff of other programs who are granted access to the data.
- IT/data management staff.

The number of people with access to personally identifiable information should be kept to a minimum. Access to data is determined by a staff person's role and the work needs of that role. This is known as role-based access. An individual staff person may have multiple roles.

De-identified data files should be used for analyses whenever possible. The Procedures Manual should describe when and how data files with personal identifiers are used and when de-identified data are used, and how this is determined.

Standard 1.3 Summary: Each program's Procedures Manual should describe the specific staff roles, types of data, access levels, and procedures for data access.

STANDARD 1.4 – Ensure that data security policies require ongoing reviews of evolving technologies and include a computer back-up or disaster recovery plan.

The IDB ORP Panel and representatives from the DHMH Office of Information Technology (OIT) should meet annually or as needed to review technological changes and ensure data security and confidentiality policies are adequate.

The Maryland DHMH maintains a secondary, secure, off-site computer operation that can be made operational in the event of a catastrophic failure at the primary location.

Programs should have a disaster recovery plan that describes how data are stored securely at an off-site location and how they can be accessed securely in the event of a catastrophic failure at the primary location.

Standard 1.4 Summary: Each program should describe its disaster recovery plan in its Procedures Manual.

STANDARD 1.5 – Ensure that any breach of data security protocol, regardless of whether personal information was released, is reported to the ORP and investigated immediately. Any breach that results in the release of personally identifiable information to unauthorized persons (breach of confidentiality) should be reported to the ORP, to the federal funding agency, and, if warranted, to law enforcement agencies.

There are two levels of breaches, a breach of data security protocol in which there is a departure from established data security policies or procedures, and the more serious breach of confidentiality in which there has been a release of personally identifiable information.

Any breach of data security protocol, regardless of whether there was a breach of confidentiality, is to be immediately reported to the person who failed to adhere to protocol and to their supervisor. All breaches are to be investigated immediately by the supervisor and/or the ORP to assess causes and implement remedies to prevent future similar breaches. The date and a description of the breach of security protocol are to be entered into a Breach Log, which is periodically reviewed by the ORP. The ORP addresses repeated breaches of data security protocol by the same employee in a counseling session with the employee and their supervisor. Additional failures to adhere to protocols after counseling are subject to reprimand and/or other disciplinary actions at the discretion of the ORP and in consultation with personnel procedures.

Any breach of confidentiality, the release of personally identifiable information to unauthorized individuals (with or without harm to one or more individuals) is to be reported immediately to the ORP. The ORP should take immediate steps to identify the extent of the breach and to contain the breach. A breach of confidentiality is also likely to involve one or more breaches of data security protocol and should be investigated appropriately. The ORP, in consultation with legal counsel, is responsible for determining if the severity of the breach of confidentiality warrants personnel or legal action in accordance with state and federal laws. If required by the federal funding source, the ORP should promptly notify the funding agency of breaches of confidentiality.

Staff members should be made familiar with the definitions of breach of data security protocol and breach of confidentiality (see Glossary) during the annual data security and confidentiality training.

Standard 1.5 Summary: Each program should describe its process for handling breaches of data security protocol and breaches of confidentiality in the Procedures Manual.

STANDARD 1.6 – Ensure that staff members with access to personally identifiable information attend data security and confidentiality training annually.

New program staff with access to personally identifiable information (including contractors) should receive training in data security and confidentiality policies and procedures during the first days of their employment. The training should cover the CDC Guidelines, as well as the IDB Guidance and the program's Procedures Manual on physical and electronic data security procedures, confidentiality procedures, and data release procedures. Training is to be repeated for all program staff on an annual basis, regardless of whether or not they are assigned activities involving personally identifiable information as part of their daily responsibilities.

Information technology (IT) staff responsible for providing technical support to equipment used to work with personally identifiable information should also complete annual trainings.

Other support staff (mail room, custodial staff, and maintenance staff) with access to personally identifiable information and the areas where this information is stored should also complete annual trainings relevant to their level of access.

Programs should consider including language on following data security and confidentiality procedures in job descriptions and employee evaluation instruments. All trained personnel should acknowledge that they have been informed, trained and provided access to a copy of the IDB Guidance and the program's Procedures Manual by signing their confidentiality pledge each year. Attendance at training sessions should be documented in personnel files.

Training should cover:

- Personal responsibilities
- Procedures for ensuring physical security of personally identifiable information
- Procedures for electronically storing and transferring data
- Procedures for data sharing
- Procedures for reporting and responding to data security breaches
- Review of relevant laws and regulations

Standard 1.6 Summary: Each program should describe its procedures for data security and confidentiality training in its Procedures Manual.

STANDARD 1.7 – Require all newly hired staff members to sign a confidentiality agreement before being given access to personally identifiable information; require all staff members re-sign their confidentiality agreements annually.

All IDB staff should annually sign an IDB confidentiality pledge (Appendix A). Individual programs may also have a program-specific confidentiality pledge (included in program Procedures Manuals). All staff authorized to access personally identifiably information (including newly hired staff) should receive appropriate training and must sign a confidentiality pledge before access to data is granted. The new employee or newly authorized staff should show the signed confidentiality statement to the grantor of passwords and keys before passwords and keys are assigned. This confidentiality pledge indicates that the employee understands and agrees that personally identifiable information should not be released to any individual not granted access by the Procedures Manual or the ORP. The original statement must be held in the employee's personnel file and a copy given to the employee.

When staff members leave employment or are no longer authorized access, keys and pass-cards to buildings and offices should be retrieved, entrance codes to limited access areas should be changed, computer accounts should be closed, and data files with personally identifiable data that are password protected or encrypted should have their passwords changed.

Standard 1.7 Summary: Each program must include any program-specific confidentiality pledges or procedures in its Procedures Manual.

STANDARD 1.8 – Ensure that all personnel authorized to access personally identifiable information take responsibility for 1) implementing the program's data security policies and procedures, 2) protecting the security of any device in their possession on which personally identifiable public health data are stored, and 3) reporting suspected security breaches.

All staff members who are authorized to access personally identifiable information are to be informed of the IDB Guidance and their program's Procedures Manual and their data security and confidentiality responsibilities.

Programs should ensure that:

- Staff are to be responsible for assuring that appropriate safeguards are in place for assigned devices that contain personally identifiable information (e.g. computer workstations, laptops, and external storage devices).
- Each employee who is issued a key/entrance code/password is to be held responsible for its safekeeping and protection. Staff are to be instructed on ways to protect keys, passwords, and codes that would allow access to personally identifiable information. All personally identifiable information is to be removed from sight on desktops and computer stations when the employee leaves their workstation for any reason.
- Staff are to be instructed on the appropriate use of personal computers and storage devices, as well as the appropriate removal of data from secure facilities.
- Staff are to be instructed on how to recognize and report suspected data security breaches and how to report breaches.
- Each staff member with access to secure areas is to be held responsible for challenging potentially unauthorized uses of data by informing their supervisor and/or the ORP.
- Staff should take care not to infect computer software and hardware with computer viruses and not to damage hardware through exposure to extreme heat or cold.

Standard 1.8 Summary: Each program should include a description of their security and confidentiality training in its Procedures Manual.

STANDARD 1.9 – Certify annually that all data security standards have been met.

Each program annually identifies the ORP and certifies that all data security and confidentiality program requirements are being met.

The process to do this involves providing a statement that:

- Identifies the ORP
- Attests to the program's adherence to data security and confidentiality standards
- Cites program-specific procedures used to document adherence to the standards

If any standards cannot be met, reasons are to be documented and plans to address these standards are to be outlined. Programs should work collaboratively with the IDB ORP Panel and federal funding agencies to address any problem areas. When standards are not met, strategic plans for the future of the program and their physical space should take these standards into account and make accommodations to meet them.

Standard 1.9 Summary: Each program should include a copy of its annual security statement in its Procedures Manual.

2.0: Data Collection and Use

STANDARD 2.1 – Clearly specify the purpose for which the data will be collected.

Programs are responsible for fully describing the intended public health purposes for data collection and the scope and limits of the data collection activities when data are shared or used.

Each program should include information regarding:

- Data involved
- Purpose and rationale of the data collection(s)
- Legal authority to collect the data, if applicable
- How data collection will likely lead to a reduction in morbidity and mortality rates through targeting of public health interventions without creating undue burdens.
    - How data collection and sharing are routinely evaluated for their ability to enhance the capacity to reduce morbidity and mortality or direct resources for prevention, treatment or other public health interventions.
- How data collection significantly differs from other approved public health data collections.
- Limits on how data may be used or shared.

Standard 2.1 Summary: Each program should include in the Procedures Manual the program-specific information on the purpose for which the program collects data.

STANDARD 2.2 – Collect and use the minimum information needed to conduct specified public health activities and achieve the stated public health purpose.

Data elements collected and shared should be:

- Reasonable and likely to achieve the stated public health goal
- Similar enough to those collected through previous data collection efforts to allow necessary comparisons.

Minimum information necessary is defined as the minimum amount of demographic, geographic, and health-related data necessary to accomplish the public health goals of the program and its affiliated programs and will vary across program areas and activities.

The minimum information necessary for collection may be specified by authorizing laws and regulations and is implemented by the data collection instruments available.

The minimum information necessary for sharing is specified in the Data Sharing Agreements between programs and will vary across program areas and activities.

Standard 2.2. Summary: Each program should include its definition(s) for minimum information necessary to perform each of its public health activities in the Procedures Manual.

STANDARD 2.3 – Collect personally identifiable information only when necessary; use de-identified data whenever possible.

Personally identifiable information is defined as: “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.”

Collection and use of personally identifiable information is justifiable if the data are to be used for a public health purpose that cannot be achieved through the use of de-identified data. Personally identifiable information requires a higher standard of data protection than de-identified data.

The following guiding questions should be considered prior to using identifiable information:

Is the use of personally identifiable information necessary to achieve the public health goal of the proposed data collection?

Have possible alternatives to using personally identifiable information, such as using anonymized data, been explored?

What are the risks and benefits of using personally identifiable information?

What is the scientific reliability and validity of personally identifiable information when used for the purposes proposed?

Can personally identifiable information be separated from other sensitive information by use of a meaningless common identifier?

Is the use of personally identifiable information required by law?

Standard 2.3 Summary: Each program should describe in its Procedures Manual why the collection of personally identifiable information is justifiable and describe the use of any alternatives to personally identifiable information.

STANDARD 2.4 – Ensure that data that are collected and/or used for public health research are used in accordance with stipulations in Common Rule, Title 45, Part 46, of the Code of Federal Regulations (CFR), which includes obtaining both institutional review board (IRB) approval for any proposed federally funded research and informed consent of individuals directly contacted for further participation.

Research is defined in 45 CFR Part 46 as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program which is considered research for other purposes. For example, some demonstration and service programs may include research activities."

The CDC often issues research or non-research determinations for funded projects. A CDC non-research determination may be based on the lack of direct CDC contact with the research participants or with their personally identifiable information. Therefore, CDC funded projects with a non-research determination may still be considered research by the DHMH IRB.

The use of personally identifiable information for research purposes should be contingent on:

- Demonstrated need for the data.
- IRB approval.
- The signing of a confidentiality statement regarding rules of access and final disposition of the information.

Release of IDB data for research purposes requires the approval of the PHPA Director or Deputy Director, or their designees, and the program's ORP. In addition, the IRB is responsible for reviewing and approving all proposed research projects involving human subjects, covered by 45 CFR Part 46, occurring in any health department program. Projects involving data collection in which there is identifiable linkage to the subject or involving physical, social, psychological, or privacy risks to the subject require IRB review. The IRB is charged with the responsibility of determining if a project qualifies as being exempt from IRB review requirements. Review of proposals by PHPA/IDB and the IRB are two separate processes, and approval of a project by the PHPA Director is required prior to IRB review.

Standard 2.4 Summary: Each program should identify any current research projects, their research partners, and the status of any IRB reviews in its Procedures Manual.

3.0: Data Sharing and Release

STANDARD 3.1 – Limit sharing of confidential or personally identifiable information to those with a justifiable public health need; ensure that any data-sharing restrictions do not compromise or impede public health program or disease surveillance activities and that the ORP or other appropriate official has approved this access.

This standard applies to the sharing of data between programs covered by the IDB Guidance as well as between these programs and other public health entities that might need routine access to the data for a related public health function. An example of data sharing between two IDB programs is the TB control and HIV surveillance programs that routinely match case registries to update case information and require reciprocal access to each other's information. An example of data sharing between an IDB program and another public health entity is the verification of eligibility for benefits between the HIV health services program and the medical assistance (Medicaid) program.

Such access should be authorized by the ORPs of the programs and the appropriate officials of the other entities maintaining the data and should be limited to the minimum numbers of persons and minimum amount of information necessary.

The program ORPs and appropriate officials should verify the:

- Appropriateness of sharing
- Integrity of the information shared
- Identity of the recipient
- Security of the method through which the information will be shared

A Data Sharing Agreement should address these points, be in writing, and be signed by the ORPs of the programs and the appropriate officials of other entities.

Standard 3.1 Summary: Each program should identify any Data Sharing Agreements with other programs and entities and provide copies of the Data Sharing Agreements in its Procedures Manual.

STANDARD 3.2 – Assess the risks and benefits of sharing personally identifiable information for other than their originally stated purpose or for purposes not covered by existing policies.

Prior to sharing personally identifiable information for other than the originally stated purpose or for purposes not covered by existing policies:

- Options for and alternatives to sharing such data for the intended public health purposes are to be explored.
- The public health purpose(s) for which data are to be used are established.
- Methods for ensuring data security and confidentiality are established.
- It is determined if sharing of personally identifiable information is necessary.
- It is ensured that the proposed purpose for which data is to be used within the scope of the program's data release policy.
- An assessment of the data security and confidentiality provisions is conducted and it is ensured that the provisions are adequate.
- It is ensured that the program or other entity receiving personally identifiable information has data security and confidentiality standards in place that are at least as stringent as those outlined in this IDB Guidance.

Standard 3.2 Summary: Each program should describe its process for assessing risks and benefits of sharing personally identifiable information in its Procedures Manual.

STANDARD 3.3 – Ensure that any public health program with which personally identifiable information is shared has data security standards equivalent to those in this document.

Data security and confidentiality can be compromised if programs or other entities that lack adequate standards to protect the security and confidentiality of public health data are granted access to such data.

Programs should share data only after the ORP(s) has weighed the benefits and risks of allowing access.

Programs should share data only with programs and other entities that have written policies and procedures establishing data security and confidentiality protections equivalent to those in the IDB Guidance.

IDB programs should review the procedures of affiliated programs during periodic site visits and/or program reviews when data security and confidentiality procedures can be discussed.

Standard 3.3 Summary: Each program should describe in its Procedures Manual the procedures for reviewing the security procedures of programs and other entities with which they have data sharing agreements.

STANDARD 3.4 – Ensure that public health information can only be used for purposes related to public health, except where required by law.

The sharing of personally identifiable information with officials in law enforcement, immigration control, or public welfare management should be justified by an imminent threat to individuals or populations or other compelling circumstance.

Any request for public health data for law enforcement purposes should be reviewed by the overall responsible party (ORP) and legal counsel of the program or programs controlling the data to determine what specific data, if any, should be released.

All possible alternatives to the use of personally identifiable information are to be examined prior to the release of such data.

Legal analysis should be conducted to determine whether the release of personally identifiable information is either prohibited or required. It should be determined if judicial oversight, the issuance of a warrant, or other protections are necessary to protect the rights of individuals whose personally identifiable information was shared.

When information is ordered released as part of a judicial proceeding, any release or discussion of information should occur in closed judicial proceedings, if possible. Maryland law prohibits the release of most surveillance data for civil lawsuits except with a court order sealing the record, and prohibits the release of any HIV surveillance information for civil lawsuits. Requests for surveillance information for criminal cases should be directed to the ORP who should consult the DHMH Assistant Attorney General to determine the appropriate response.

Standard 3.4 Summary: Each program must describe in its Procedures Manual the non-public health uses of its data that are required or permitted by law.

STANDARD 3.5 – Establish procedures, including assessment of risks and benefits, for determining whether to grant requests for aggregate data not covered by existing data-release policies.

Any sharing of aggregate data should be for a legitimate public health purpose and in accordance with applicable laws and regulations.

Precautions are to be taken to ensure that the disseminated data are not presented in ways that may indirectly identify individuals. Programs should develop procedures that restrict release of certain data elements or cells of data below a specified size as some aggregate data could be used to identify individuals. However, the obligation to use data to help members of demographic groups may outweigh the risk of possible identification of group members, as well as the potential community-wide stigma that could be associated with some aggregate data.

All new requests for aggregate data are to be submitted to the program for review, the program should weigh the risks and benefits of each request prior to dissemination of data.

Programs should have written procedures for determining whether and how to grant requests for aggregate data not covered by currently implemented data release policies.

Standard 3.5 Summary: Each program should describe in its Procedures Manual the procedures for responding to requests for releases of aggregate data.

STANDARD 3.6 – Disseminate de-identified aggregate data to stakeholders as soon as possible after data are collected.

De-identified data should be disseminated to stakeholders regularly. Procedures should be established by each program to disseminate aggregate data in a manner that facilitates understanding by affected populations.

Program policies for dissemination of information can be found in the data release policy discussed in STANDARD 3.8.

Standard 3.6 Summary: Each program should describe its plan and timeline to routinely disseminate de-identified aggregate data in the Procedures Manual.

STANDARD 3.7 – Assess data quality before disseminating data.

Prior to dissemination:

- Data should be evaluated for completeness, validity, reliability, and reproducibility during collection, management, analysis, and use.
- Mechanisms should be in place to evaluate the usefulness of disseminating data to stakeholders.
- Data products should be cleared by appropriate officials before their publication or release.

Guidance on ensuring data quality is provided in the HHS Guidelines for Ensuring the Quality of Information Disseminated to the Public, Part D, CDC and the Agency for Toxic Substances and Disease Registry (ATSDR)

http://www.cdc.gov/maso/qualitycontrol/Guidelines.htm

Standard 3.7 Summary: Each program should describe in its Procedures Manual the current procedures for ensuring data quality prior to dissemination.

STANDARD 3.8 – Ensure that data-release policies define purposes for which the data can be used and provisions to prevent public access to raw data or data tables that could contain indirectly identifying information.

Each IDB program should develop a set of procedures for handling data releases. The procedures should include information regarding:

- Roles and responsibilities of program personnel, including:
  - Confidentiality agreements they should sign
  - Training they should receive
- Description of purposes for which the data can be used.
- Access procedures and authorization rules.
- Descriptions of the data.
- Descriptions of to whom data can be released, and in what format.
- Procedures for data release.
- Specific requirements for sharing personally identifiable information.
- Mechanisms for data release, including rules for minimizing disclosure such as cell-size restrictions.
- Disposition of data after they have been used for a stated purpose.
- Provisions to prevent public access to raw data or data tables that could contain indirectly identifying information.
- Mechanisms for evaluating the usefulness of released data and whether the release of data is causing undue burden on individuals or communities.
- Description of the physical and electronic controls that should be used to manage data releases securely.
- General IT procedures or references to IT policies that protect data.
- Mechanisms and procedures for requesting data and considering data requests.
- Suggested formats for data-use agreements should be described.

Standard 3.8 Summary: Each program should describe in its Procedures Manual the procedures for handling data releases.

4.0: Physical Security

STANDARD 4.1 – To the extent possible, all personnel working with paper or electronic copies of documents containing confidential, personally identifiable information do so within a secure locked area.

All programs should meet the following minimum requirements for secure areas:

- Work space with limited access only for necessary staff
- Locked file cabinets that are large and heavy enough to render them immobile
- A designated location within the work space where confidential conversations may be held

If data are to be stored or used in less than optimal secure work areas, the security of these areas should be improved as much as possible. For example, in many workplaces confidentiality is improved by requiring paper documents with confidential information to be kept locked in desk drawers when not in use or when a worker is away from his or her desk. Data security might also be improved by reconfiguring cubicles, office partitions, and requiring confidential phone conversations to take place in a private room.

Programs should strive to meet the following enhanced data security and confidentiality configurations:

- A dedicated, secure area accessible only via locked door with limited key or keycard distribution to minimal staff
- Double-locked file cabinets that are large and heavy enough to render them immobile
- A workstation/table equipped with a telephone and computer to handle data within the secure space

When possible, servers and workstations should be on a closed local area network (LAN) that is accessible only to authorized personnel. If limited local resources require that personally identifiable information be stored on a LAN that is accessible by unauthorized personnel, real-time encryption software that meets federal encryption standards should be employed. Any time a computer workstation that contains personally identifiable information is left unsupervised, authorized personnel should log off to ensure that unauthorized individuals cannot access the data.

Policies for Work Off-Site

Some situations may require staff to work with personally identifiable information off-site through tele-work, field work, or remote work. This may include both paper documents and electronic data. Appropriate measures should be taken to ensure that personally identifiable information is kept as securely as is reasonably possible given the nature of the situation.

When dealing with personal identifying information off-site the following minimum standards for electronic security should be followed:

- The media device being used to store personally identifiable information should be fully encrypted (encryption of individual files is not sufficient).
- No personally-owned computers or electronic data storage media may be used. The device should be issued by the agency. An outside internet service provider or personal network equipment may be used for internet connectivity on the agency's device.
- Agency computers should be configured to not allow installation of software by anyone other than agency IT staff.
- The agency should have properly configured firewalls installed on computers that are to be used outside of the agency's protective boundaries.
- Personal identifying information should never reside on a device that is ever connected to the internet either directly or indirectly outside of the agency firewall.
- Personal identifying information may be analyzed only if technology is used to access and analyze remotely with only displays of data and results being shown on the device.

State Regulations (COMAR 17.04.11.02 B9 (1)(a) which can be found at http://www.dsd.state.md.us/comar/comarhtml/17/17.04.11.02.htm) permit Appointing Authorities to determine tele-work participation. Tele-working is an arrangement between an employee and the employee's supervisor which allows the employee to work at home, a satellite office, or at a Tele-work Center on selected work days. The PHPA tele-work policy specifies that employees who deal with personally identifiable information or documents, as determined and defined by the Center or Office Chief and the PHPA Director or Deputy Director, should only work at a PHPA approved secure satellite office or home office. Tele-work participation by IDB employees is only permitted in specific situations approved by the IDB Director.

Approved tele-work environments in which personally identifiable information are used should meet the same data security and confidentiality protections as the office work space. Minimally, such tele-work locations should:

- Have work space with limited access in a private area (e.g. a locked, dedicated room in a home that is not accessible by unauthorized individuals).
- Not have hard-copy storage of personally identifiable information. If hard copies of documents are stored in a tele-work site, they should be stored in double locked file cabinets large and heavy enough to be rendered immobile. Hard copies should never be left in an unsecured area and should be shredded using a cross-cut shredder before disposal.
- Be configured to allow confidential conversations.

- Use a computer with encryption software at least equal to the currently accepted level of encryption used in the regular workplace to store and transmit personally identifiable information.
- Use a secure Wi-Fi connection if the computer is connected to the internet via Wi-Fi.

Personnel may need to carry some identifying information when doing field or clinic work. Policies related to the use of personally identifiable information in field work can be found in Standards 4.5 and 4.6 in this IDB Guidance and program-specific procedures can be found in the corresponding sections of the programs' Procedures Manuals.

In the case of emergency or outbreak responses, staff may also be detailed to remote work sites that have not been prepared to meet ideal secure space criteria. In those cases, host area and detailed staff should ensure that the work site is made as secure as reasonably possible in terms of physical, electronic, and procedural data security. Optimally, remote work spaces should:

- Have partitions of at least 6 feet, if possible, especially around the perimeter of the areas.
- Place staff in the center of the area, leaving vacant cubicles around the perimeter to provide a buffer.
- Have an enclosed room or other relatively private area where confidential phone conversations can be conducted.
- Have work space with limited access in a private area (e.g. a locked, dedicated room in a home that is not accessible by unauthorized individuals).
- Not have hard-copy storage of personally identifiable information. If hard copies of documents should be stored in a remote work site, they should be stored in double locked file cabinets large and heavy enough to be rendered immobile. Hard copies should never be left in an unsecure area and should be shredded using a cross-cut shredder before disposal.
- Use a computer with encryption software at least equal to the currently accepted level of encryption used in the regular workplace to store and transmit personally identifiable information.
- Use a secure Wi-Fi connection if the computer is connected to the internet via Wi-Fi.

Standard 4.1 Summary: Each program should describe in its Procedures Manual the physical security for its work areas. If these do not meet the minimum requirements for secure areas, then the measures taken to minimize security risks should be described. Each program should also describe, if applicable, its procedures for home and field offices.

STANDARD 4.2 – Ensure that documents containing personally identifiable information are shredded with crosscutting shredders before disposal.

Any hard copies containing personally identifiable information that are no longer needed are to be shredded in a commercial-quality crosscutting shredder prior to disposal.

Contracting with a document-shredding service may be an option for some programs. If a service is used, documents should be shredded on site and in the presence of a staff member. In all cases, a contract shredding or disposal company should be bonded, and due diligence should be taken in the selection of the company.

The IDB has a records retention and disposal schedule (DHMH Schedule #2294, 2003) [update submitted in 2012, not yet finalized].

See National Institute of Standards and Technology Special Publication 800-88, Guidelines for Media Sanitation, available at http://csrc.nist.gov/publications/ for discussion of shredding and destruction of paper and other media

Standard 4.2 Summary: In its Procedures Manual, each program should describe in detail the components of the IDB records retention and disposal schedule that apply to their program. Each program should describe its procedures for shredding paper documents that are no longer needed.

STANDARD 4.3 – Ensure that data security policies and procedures address handling of paper copies, incoming and outgoing mail, long-term paper storage, and data retention. The amount of personally identifiable information in all such correspondence should be kept to a minimum and destroyed when no longer needed.

Minimum information varies for activities and projects but is in compliance with laws, policies and procedures.

Staff members should minimize the amount and sensitivity of information contained in any piece of correspondence.

For data transmissions, the use of terms easily associated with infectious diseases should be avoided when possible anywhere in the data transmission, including sender and recipient addresses and labels.

If electronic copies exist, paper copies are to be destroyed when no longer needed, in accordance with established health department policies.

After use, hard copies of any correspondence regarding public health data are to be shredded using a crosscutting shredder as described in Standard 4.2.

Standard 4.3 Summary: Each program should describe in its Procedures Manual the current policies and procedures regarding the handling of incoming and outgoing mail and paper copies of personally identifiable information.

STANDARD 4.4 – Limit access to secure areas that contain personally identifiable information to authorized persons, and establish procedures to control access to secure areas by non-authorized persons.

Access to secured areas that contain personally identifiable information should be limited to authorized individuals.

Specific procedures should be in place to allow "guests" to enter secure areas when necessary. A guest is any person who does not have authorized access to personally identifiable information, has not been given access codes to a secure area, and whose name is not listed on the authorized staff list (this includes visitors and cleaning or maintenance personnel). All guests should be escorted by authorized staff when entering a secure area. Any person escorting a visitor into a secure area should sign-in and sign-out the guest by name on the visitors log. Cleaning staff or maintenance personnel are to be admitted to secure areas only under supervision of authorized staff. During such times, an authorized staff member should note in the visitors log "Housekeeping" or "Maintenance" and the time they enter and exit the secure area. Staff should announce the presence of any guest to all staff when the guest enters. Be sure that all personally identifiable information is out of view and that staff are not holding conversations using personally identifying information. Maintenance and security personnel may need to enter after business hours in emergency situations, in which case the ORP is to be notified on the next business day.

Standard 4.4 Summary: In its Procedures Manual, each program must describe who has access to its secure areas and how guest access is controlled and documented.

STANDARD 4.5 – Ensure that program personnel working with documents containing personally identifiable information in the field: 1) return the documents to a secure area by close of business, 2) obtain prior approval from the program manager for not doing so, or 3) follow approved procedures for handling such documents.

Specific physical measures should be taken if documents containing personally identifiable information are taken to personal residences or other locations. Case reports and other confidential materials are to be hand carried in one of two ways: 1) inside a locking container (such as a briefcase or bag) or 2) with case information and identifiers separated and sealed in separate envelopes. In both scenarios, the materials are to be in the possession of the authorized staff member at all times and should be returned to a secure area by the close of business. Business travel situations that require personally identifiable information to be kept out of the office overnight require prior approval from the ORP.

Personally identifiable information should not routinely be taken to private residences. There are three exceptions: 1) when out-stationed staff who on occasion, due to the geographic location of their residences, field offices and the main office, have to take personally identifiable information to their residence in order to hand carry it to the main office the next business day, 2) when travel to outlying areas precludes the return of personally identifiable information to the field offices before close of business, and 3) when inclement weather or a local, state, or national emergency situation precludes the return of personally identifiable information to the main or field offices. During these instances, the information should be kept secure at all times inside locked briefcases.

Standard 4.5 Summary: Each program should describe in its Procedures Manual, the procedures for reviewing and approving situations where personally identifiable information is not returned to a secure area at night.

STANDARD 4.6 – Ensure that documents with line lists or supporting notes contain the minimum amount of personally identifiable information necessary and, if possible, that any personally identifiable information is coded to prevent inadvertent release of personally identifiable information.

When identifying information (either in hard copy or electronically) included on line lists or supporting notes are taken from secured areas for necessary public health activities, documents should contain only the minimum amount of information necessary to complete the given task.

Any personally identifiable data elements and items that would associate the information with specific infectious diseases should be removed (e.g., descriptive variable names) or coded.

Standard 4.6 Summary: Each program should describe in its Procedures Manual, the procedures for minimizing or coding personally identifiable information that is taken into the field.

5.0: Electronic Data Security

Implementation of electronic data security standards are conducted in a rapidly evolving technological environment. While technology is changing, the elements of access, encryption, backups, and secure transmissions will remain important to consider when developing policies. See the CDC Guidelines pages 28-29 for more detailed discussion about these elements.

STANDARD 5.1 – Ensure that analysis data sets that can be accessed from outside the secure area are stored with protective software (i.e., software that controls data storage, removal, and use), and verify removal of all personal identifiers.

Analysis of data sets with personally identifying information are to be performed in secure areas only, unless approved by the ORP in special cases. Data sets taken out of secure areas for the purpose of analysis should be stripped of personally identifying information (de-identified). Analysis data sets should include only the minimum number of sensitive or potentially linkable data elements needed for analysis. The minimum amount of data required is defined on a case by case basis or in Data Sharing Agreements. Access to analysis data sets should be restricted through methods such as restricted access folders, storage on portable media, and encryption.

Roles are to be assigned to selected individuals to create analysis data sets to minimize the number created (see Standard 1.3).

Standard 5.1 Summary: Each program should describe, in its Procedures Manual, the procedures for creating, storing, protecting, and destroying any analysis data sets accessed outside the secure area.

STANDARD 5.2 – Ensure that any electronic transfer of data is approved by the ORP and subject to access controls, and that personally identifiable information is encrypted before being transferred.

All electronic transfers of data should be approved by the ORP and subject to access controls. Personally identifiable information should be encrypted before being transferred electronically. Ideally, electronic transfers of data should use a secure connection such as a secure data network (SDN) or virtual private network (VPN) with certification on both ends. At a minimum, data are to be encrypted and sent using a secure application such as a file transfer protocol (FTP) with certification on at least one end.

Whenever possible, databases and files with individual-level data are to be encrypted when not in use. Electronic files being stored for future use (e.g., ancillary databases and working laboratory datasets) should be encrypted until they are actually needed.

Data extracts from sources outside the health department, including hospitals and laboratories, should meet the minimum data security standards used within the health department. Approved data transfer methods should be used when designing electronic reporting mechanisms for laboratories, providers, etc.

Additional resources on electronic data exchange can be found at http://www.cdc.gov/ehrmeaningfuluse/ and the public health information network (http://www.cdc.gov/phin/).

Standard 5.2 Summary: Each program should describe in its Procedures Manual the procedures for electronic data transfers and the procedures for securing and storing data sets that are not in use.

STANDARD 5.3 – Before transferring electronic data containing personally identifying information, ensure that the data have been encrypted with use of an encryption package that meets Advanced Encryption Standard (AES) criteria and that the data transfer has been approved by the appropriate program official or ORP. No electronic data containing identifying information should be transferred without being encrypted.

Data containing personally identifying information are to be encrypted in line with federal encryption standards before being transferred electronically. The preferred method of securing data is with whole-device encryption that fulfills FIPS 140-2 standards available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Individual-level data that does not contain personally identifying information can be transferred electronically without meeting federal encryption standards with the approval of the ORP, but terms associated with infectious diseases should not appear anywhere in the context of the transmission.

Personally identifiable information should not be sent or received via email when it can be avoided, and should be encrypted. Transfer via more secure electronic transfer methods, such as secure FTP transfers (SFTP), personal communication, or legally protected hard-copy mail delivery is preferable. Partners and providers who submit personally identifiable information to the health department should be informed of acceptable methods of transfer.

Facsimile transmissions are addressed in Standard 5.5.

Standard 5.3 Summary: In its Procedures Manual each program should outline its procedures regarding transfer of personally identifiable information by electronic methods. If a program's procedures permit personally identifiable information to be transferred by email, they should describe in detail the circumstances under which it is permissible and what procedures are in place to minimize the risk of the data being viewed by unauthorized individuals.

STANDARD 5.4 – Use encryption software that meets federal AES standards to encrypt data with personal identifiers on all laptops and other portable devices that receive or store public health data with personal identifiers.

Data sets with personally identifiable information should only be received or stored on laptops and other portable or external storage devices when necessary, as defined by each program's Procedures Manual, and should be encrypted. Encryption of analysis data sets is not required if personally identifiable information have been removed; however, encryption is recommended to protect from accidental or intentional misuse.

Removable or external storage devices or hard drives containing personally identifiable information should:

- Include only the minimum amount of information necessary to accomplish assigned tasks as determined by the designated official or ORP;
- Be separated from the laptop, and encrypted or stored under lock and key when not in use; and
- Be sanitized immediately following the assigned task (except for those used as data back-ups) so that data may not be retrieved.

Decryption keys or passwords are not to be stored on the laptop or external storage device. Out-of-service hard drives and electronic media are to be stored in a secure area until they are sanitized and/or physically destroyed. Hard drives or other storage media once containing personally identifiable information should be sanitized prior to being sent off site for repair.

Picture taking in areas where personally identifiable information is in use is prohibited. Photos may only be taken outside of secure areas and away from personally identifiable information. This applies to pictures taken using cameras, cells phones, PDAs, or any other device.

Programs may review National Institute of Standards and Technology Special Publication 800-124, Guidelines on Cell Phone and PDA Security, available at http://csrc.nist.gov/publications/) when developing policies.

Standard 5.4 Summary: Each program should describe in its Procedures Manual when personally identifiable information may be stored on laptops and other portable devices, how the information is protected, and how to sanitize or physically destroy storage devices when tasks are completed.

STANDARD 5.5 – Ensure that data policies include procedures for handling incoming and outgoing facsimile transmissions. Minimize inclusion of personally identifying information in fax transmissions, and destroy hard copies and sanitize hard drives when no longer needed.

The faxing of personally identifiable information is allowed but should be avoided when possible. Transfer via more secure electronic transfer methods, such as secure FTP transfer, personal communication, or legally protected hard-copy mail delivery is preferable. Partners and providers who submit personally identifiable information to the health department should be informed of acceptable methods of transfer.

If faxing is necessary, program-specific procedures should be in compliance with Appendix F of the CDC Guidelines.

Standard 5.5 Summary: Each program should outline in its Procedures Manual, the procedures regarding transfer of personally identifiable information via fax. If a program's procedures permit personally identifiable information to be transferred by fax they should describe in detail the circumstances under which it is permissible and what procedures are in place to minimize the use of faxing to transfer data, to minimize the amount of personally identifiable information contained in the transfers, and to minimize the risk of the data being viewed by unauthorized individuals.

Each program should describe its procedures for storing paper copies of faxes and for destroying them when no longer needed.

Each program should describe its procedures for destroying or sanitizing any printing materials or hard drives in the fax machine that may contain images of confidential data.

References and Resources

Advanced Encryption Standard (AES):
Publications 197 and 140-2 of the Federal Information Processing Standards (FIPS) (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

CDC Program Collaboration and Service Integration (PCSI):
Centers for Disease Control and Prevention. Program Collaboration and Service Integration: Enhancing the Prevention and Control of HIV/AIDS, Viral Hepatitis, Sexually Transmitted Diseases, and Tuberculosis in the United States. Atlanta (GA): U.S. Department of Health and Human Services, Centers for Disease Control and Prevention; 2009.

CDC Data Security and Confidentiality Guidelines:
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.

Cell Phone and PDA Security:
National Institute of Standards and Technology Special Publication 800-124, Guidelines on Cell Phone and PDA Security (http://csrc.nist.gov/publications/)

CSTE Webinar Series:
Implementing the Integrated Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Diseases, and Tuberculosis Programs. Council of State and Territorial Epidemiologists; 2013. (http://www.cste.org/?page=WebinarLibrary)

Ensuring Data Quality:
Centers for Disease Control and Prevention, Agency for Toxic Substances and Disease Registry. Guidelines for ensuring the quality of information disseminated to the public. http://www.cdc.gov/maso/qualitycontrol/Guidelines.htm. Accessed November 11, 2011.

NIST Contingency Planning Guide for Federal Information Systems:
National Institute of Standards and Technology Special Publication 800-34, Contingency Planning Guide for Federal Information Systems (http://csrc.nist.gov/publications/PubsSPs.html)

NIST Guide to Protecting Confidentiality of Personally Identifiable Information:
National Institute of Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (http://csrc.nist.gov/publications/)

NIST Guidelines for Media Sanitation:
National Institute of Standards and Technology Special Publication 800-88, Guidelines for Media Sanitation (http://csrc.nist.gov/publications/)

Resources on Electronic Data Exchange:
http://www.cdc.gov/ehrmeaningfuluse/
http://www.cdc.gov/phin/

List of Acronyms

AES	Advanced Encryption Standards
AIDS	Acquired Immunodeficiency Syndrome
ATSDR	Agency for Toxic Substances and Disease Registry
CBO	Community Based Organization
CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CHPHS	Center for HIV Prevention and Health Services
CHSEE	Center for HIV Surveillance, Epidemiology and Evaluation
CI	Center for Immunization
COMAR	Code of Maryland Regulations
CPQI	Center for Planning and Quality Improvement
CSIPOR	Center for Surveillance, Infection Prevention, and Outbreak Response
CSTE	Council of State and Territorial Epidemiologists
CSTIP	Center for STI Prevention
CTBPC	Center for TB Prevention and Control
CZVBD	Center for Zoonotic and Vector Borne Disease
DHMH	Department of Health and Mental Hygiene
EIP	Emerging Infection Program
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GA	Georgia
HHS	Health and Human Services
HIV	Human Immunodeficiency Virus
IDB	Infectious Disease Bureau
IRB	Institutional Review Board
IT	Information Technology
LAN	Local Area Network
NCHHSTP	National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention

NIST	National Institute of Standards and Technology
ODR	Office of the Director
OFBCI	Office of Faith Based and Community Initiatives
OIDEOR	Office of Infectious Disease Epidemiology and Outbreak Response
OIDPCS	Office of Infectious Disease Prevention and Care Services
OIH	Office of Immigrant Health
OIT	Office of Information Technology
ORP	Overall Responsible Party
PCSI	Program Collaboration and Services Integration
PDA	Personal Digital Assistant
PHIN	Public Health Information Network
PHPA	Prevention and Health Promotion Administration
PII	Personally Identifiable Information
SDN	Secure Data Network
SFTP	Secure File Transfer Protocol
STD	Sexually Transmitted Disease
STI	Sexually Transmitted Infection
TB	Tuberculosis
US	United States
VH	Viral Hepatitis
VPN	Virtual Private Network

Glossary – Definitions of Terms

Access: Ability or means needed to read, write, modify, or communicate data/information.

Access control: Cohesive set of procedures designed to ensure that anyone with access to personally identifiable information:

- Is the person he or she claims to be (authentication),
- Has a verified public health need to have access to the data in question, and
- Has been authorized to access the data and is doing so from an authorized place using an authorized process

Advanced Encryption Standard (AES): This standard specifies the algorithm that can be used to protect electronic data and is issued by the National Institute of Standards and Technology (NIST). Publication 197 of the Federal Information Processing Standards (FIPS) (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) contains the specifications of the AES, which can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back to its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. NIST publication 140-2 details the protection of a cryptographic module within a data security system necessary to maintain the confidentiality and integrity of the information protected by the module http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Aggregate data: Summary statistics, compiled from individual level data/ personally identifiable information, but is grouped in a manner to preclude the identification of individual cases. See **Surveillance data.**

Analysis dataset: Set of data created by removing personally identifying information (e.g., names, addresses, ZIP codes, telephone numbers) so that the data cannot be linked to a specific person but can still be used for data analysis.

Authorized access: As determined by the Overall Responsible Party (ORP) or a designee, the permission granted to individuals to see full or partial information and data that potentially could be identifying or linked to an individual. The ORP or designee should make these determinations according to role-based (or need to know) responsibilities.

Authorized personnel: Those individuals employed by the program who, in order to carry out their assigned duties, have been granted access to personally identifiable information. Authorized personnel should have a current, signed, approved, and binding nondisclosure agreement on file (confidentiality pledge).

Breach of data security protocol: A departure from established policies or procedures, or a compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of personally identifiable information. A breach is an infraction or violation of a policy, standard, obligation, or law. A breach in data security protocol would include any unauthorized use of data, even aggregated data without names. A breach may be malicious or unintentional and may or may not also include a breach of confidentiality.

Breach of confidentiality: See breach of personally identifiable information.

Breach of personally identifiable information: Defined by OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Case-specific information: Any combination of data elements that could identify a person reported to the disease monitoring system.

CDC Guidelines: 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.

Confidential information: Any information about an identifiable person or establishment, when the person or establishment providing the data or described in it has not given consent to make that information public and was assured confidentiality when the information was provided. See **Personally identifiable information (PII)**.

Confidentiality: Protection of personal information collected by public health organizations. The right to such protection is based on the principle that personal information should not be released without the consent of the person involved except as necessary to protect public health.

Confidentiality agreement (or nondisclosure agreement): A contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by third parties. It is a contract through which the parties agree not to further disclose information covered by the agreement.

Data dissemination: Any mechanism by which data (typically in aggregate form) 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.

Data encryption standard (DES): Algorithm that encrypts and decrypts data in 64-bit blocks. Since the DES always operates on data blocks of equal size and uses both permutations and substitutions in its algorithm, it is both a block cipher and a product cipher.

Data release: Dissemination of data either in a public-use file or as a result of a 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 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 steward: Person responsible for ensuring that data used or stored in an organization's computer systems are secure, classified appropriately, and used in accordance with organizational policies.

De-identified: The removal of personal data (e.g. names, addresses, ZIP codes, telephone numbers) so the record cannot be linked to an individual, but still allows the remaining data to be analyzed.

Disaster recovery: Use of off-site computer operations (where copies of data and information systems are stored) to recover data lost as the result of a catastrophe at the primary site of data storage or to activate information systems to replace those lost.

Disclosure: Occurs when personally identifiable information concerning an individual is made known to a third party. Disclosures may be *authorized* (as when a person has consented to the information being so divulged), *unauthorized* (as when information is intentionally revealed to a party not consented to by the person), or *inadvertent* (as when a tabulation or file is unintentionally made available to the public that reveals or can be used to reveal personal information).

Encryption: Manipulation or encoding of information so that only parties intended to view the information can do so.

IDB Guidance: This document. Maryland Department of Health and Mental Hygiene, Prevention and Health Promotion Administration, Infectious Disease Bureau, Data Security and Confidentiality Guidance for Infectious Disease Programs; 2013.

Individual level data: Listed data of individual case information, as opposed to aggregate data. This includes both personally identifiable information and de-identified information.

Legitimate public health purpose (see also Public health data use): 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; 4) guidance of timely, appropriate response to individual cases. Public health purposes can include analysis and evaluation of conditions of public health importance and evaluation of public health programs.

Need-to-know access: The case by case granting or denying of authorized access to case-specific information. This type of access is not routine; but rather it is for unusual situations and occurs only after careful deliberation by the ORP in concurrence with other public health professionals.

Non-public health uses of surveillance data: The release of data that is either directly or indirectly identifying to the public; to parties involved in civil, criminal, or administrative litigation; to non-public health agencies of the federal, state or local government; or for commercial uses.

Overall Responsible Party (ORP): High-ranking official who accepts overall responsibility for implementing and enforcing data security standards. This official should have the authority to make decisions about program operations that might affect programs accessing or using the data, and should serve as contacts for public health professionals regarding data security and confidentiality policies and practices. The ORP is responsible for protecting data as they are collected, stored, analyzed, and released and should certify annually that all data security program requirements are being met. Data security and confidentiality Procedures Manuals for disease programs should indicate the programs' ORP(s) by name.

Personal identifier: Information that allows the identity of a person to be determined with a specified degree of certainty. This could be a single piece of information or several pieces of data which, when taken together, may be used to identify an individual. Therefore, when assembling or releasing analysis data sets, it is important to determine which fields, either alone or in combination, could be used to identify a person and which controls provide an acceptable level of data security.

Personally identifiable information (PII): As defined by National Institute of Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), available at http://csrc.nist.gov/publications/ "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." See **Confidential information.**

Physical access controls: Physical barriers such as locked doors, sealed windows, password-protected keyboards, entry logs, guards, etc., used to help limit access to personally identifiable information.

Procedures Manual: A program-specific compilation of policies and procedures that implement the data security and confidentiality requirements of the CDC Guidelines and the IDB Guidance.

Public health surveillance: The ongoing, systematic collection, management, analysis, and interpretation of health-related data followed by their dissemination to those who need to know in order to: 1) monitor populations to detect unusual instances or patterns of disease, toxic exposure, or injury; 2) act to prevent or control these threats; and 3) intervene to promote and improve health. The term applies to both electronic and paper-based systems.

Public health data use (see also Legitimate public health purpose): Includes the variety of ways public health data may be used to achieve public health goals/purposes. A principal public health data use at state and federal levels is for epidemiologic monitoring of trends in disease incidence and outcomes. This includes collection of data and evaluation of the collection system, as well as the dissemination of aggregate trends in incidence and prevalence by demographic, geographic, and behavioral risk characteristics to assist the formulation of public health policy and direct intervention programs. Public health data uses may also include data used to initiate or provide treatment and prevention services.

Records retention policy: A policy that stipulates how long paper and electronic records should be kept before they can be archived or destroyed.

Role-based access: Access to specific information or data granted on the basis of a person's job status or authority. This control mechanism protects data and system integrity by preventing access to unauthorized applications. Granting access based on roles within an organization, rather than by individual users, simplifies an organization's data security and confidentiality policies and procedures and helps avoid granting need-to-know access to individuals.

Sanitize: The process of permanently removing, destroying, or overwriting data from electronic storage media so that the data can no longer be accessed. Some sanitization methods also prevent any future use of the electronic storage media.

Secure(d) area: Work space with physical access controls in which personally identifiable information is kept and/or used with access granted only to authorized persons. The configuration of a secure(d) area depends on resource and other program considerations (e.g., availability of physical space, locks, file cabinets, walls, doors, and other barriers.)

Security: Protection of public health data and information systems to prevent unauthorized release of identifying information and accidental loss of data or damage to the systems. Security measures include measures to detect, document, and counter threats to data confidentiality or the integrity of data systems.

Surveillance: See **Public health surveillance**.

Surveillance data: Statistics generated from a disease registry in either paper or electronic format. See **Aggregate data.**

Surveillance information: Details collected on an individual or individuals for the purpose of completing routine or special surveillance investigations. Examples of surveillance information are the disease report forms, ancillary notes about exposure investigations and related questionnaires, notes about suspect cases, laboratory reports, ICD-9/10 diagnosis line lists, discharge summaries, death certificates, and drug data records.

Syndemic: Synergist interaction of two or more conditions that contribute to an excess burden of disease in a population.

Virtual private network (VPN): Network of computers that uses encryption to scramble all data sent through the internet—making the network “virtually” private.

Appendices

Appendix A: Infectious Disease Bureau Data Security and Confidentiality Pledge

Maryland Department of Health and Mental Hygiene
Prevention and Health Promotion Administration
Infectious Disease Bureau

Confidentiality Pledge

I recognize that the following information is confidential:

The name or any other personally identifiable information (such as Social Security number) which could identify an individual who is/has been:

- Reported to IDB through its surveillance activities;
- An applicant to or client of the Maryland AIDS Drug Assistance Program or other health services program sponsored by IDB;
- An applicant to or client of any other IDB or DHMH program;
- A participant in an IDB sponsored program that targets persons with an infectious disease or at high risk for an infectious disease.

Any information that could be used to identify the disease status of an individual participating in a program sponsored by IDB or DHMH.

I will not disclose confidential information orally, in writing, or by electronic means, to anyone outside of IDB, except as required in order to complete the responsibilities of my position.

I will not disclose or discuss, any client-specific information with others in IDB, except as required to fulfill the responsibilities of my position.

I will not provide others within IDB with access to any confidential information unless they need the information in order to fulfill their work assignments and they are authorized to have the information.

I will follow the established policies of IDB to maintain confidentiality. I have received a copy of the IDB Data Security and Confidentiality Guidance and have reviewed these policies with my supervisor.

I will follow the established procedures of my disease program to maintain confidentiality. I have received a copy of the Data Security and Confidentiality Procedures Manual for my disease program(s) and have reviewed these procedures with my supervisor.

I understand that failure to follow the established policies and procedures, in order to protect confidential information known to me as a result of my work at or with IDB, will result in disciplinary action up to and including dismissal from my position and may result in civil liability and/or criminal prosecution.

PRINT NAME _____

SIGNATURE _____

DATE _____

Appendix B: Data Sharing Agreement Template

DHMH/PHPA/IDB Data Sharing Agreement Template – August 2013

Instructions

Edit the following pages to suit the needs of the data sharing activity.

Instructions are provided in square brackets: [instruction]

Capitalized text in the instructions should be replaced with appropriate language for this Data Sharing Agreement: [SHORT TITLE].

After responding to the instructions and supplying the requested text there should not be any bracketed instructions left in the final agreement.

Additional sections can be added. Please use the same format, name the sections, and underline the section names.

Specify the names of any attachments in the List of Attachments section and indicate the number of pages in each attachment or include the statement "No attachments". The attachments do not count in the number of pages in the agreement.

Edit the footnote on the first page to reflect the total number of pages in the agreement, not counting any pages in the attachments.

Delete this instruction page.

[SHORT TITLE]

Data Sharing Agreement

between

Maryland Department of Health and Mental Hygiene
Prevention and Health Promotion Administration
Infectious Disease Bureau
[PROGRAM NAME]

and

[NAME OF OTHER ENTITY]

[DATE OF DRAFT]

Introduction

This document describes a Data Sharing Agreement of confidential public health data that includes personally identifiable information between the Maryland Department of Health and Mental Hygiene, Prevention and Health Promotion Administration, Infectious Disease Bureau, [PROGRAM NAME] and [NAME OF OTHER ENTITY]. The full title of this Data Sharing Agreement is [LONG TITLE] and the short title is [SHORT TITLE or "the same" or delete this clause].

Purpose

The purpose of this Data Sharing Agreement is to [describe the purpose of the data sharing, the intent of the entity receiving the data, the types of data to be shared, the actions to be taken with the data, and the populations to be served.]

The data covered by this Data Sharing Agreement [will or will not] be used in a research study. [If used in a research study, provide details on the research protocol, funding source, and IRB approval.]

[Describe the public health benefits of the data sharing.]

[Describe the potential risks of the data sharing.]

Legal Authority

The data to be shared is collected by [the name of the entity collecting the data] under [provide legal authority to collect this data].

[Describe any legal requirements covering sharing the data.]

[Describe the legal authority of the entity to receive the data.]

[If this is a two way data exchange – then describe the authorities and requirements for both directions.]

Description

[Describe the details of the data sharing. Including topics such as: types of data (if extensive, a variable list should be included as an attachment), types of transfers or access, frequency, etc.]

[Diagrams can be helpful and inserted here or as attachments.]

[Discuss how the data to be shared is the minimum amount of personally identifiable information

needed to perform the covered public health activity.]

Method and Security of Transfer

[Describe the methods and security of the data transfers/access.]

Security of Host System

[Entities receiving data should describe their data security and confidentiality procedures relative to this data sharing activity. These procedures should address the 10 guiding principles and be in compliance with the CDC data security guidelines. A copy of the procedures should be included as an attachment.

"Ten Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality." Lee and Gostin, JAMA 2009.

"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."]

Personnel with Access

Access by individual staff to personally identifiable information will be granted based on the need for access to order to perform their job function. This is known as role-based access. Only the following types of staff will have access to the data.

[Describe the staff positions requiring access to the shared data in order to perform their jobs.]

Storage

[Describe how and where the shared data are to be stored.]

[Describe if and when the shared data are to be archived, and the mechanism to be used.]

Destruction

[Describe if and when the shared data are to be destroyed, and the mechanism to be used.]

Re-Release of Data

Data shared as part of this Data Sharing Agreement are not to be shared with any other entities,

except as described in this Data Sharing Agreement.

[Describe any sharing of this data with other entitities.]

Dissemination

Individual personally identifiable information is not to be disseminated.

Dissemination of aggregated public health data is expected and encouraged, however, the entity providing the data retains the right to review and approve all public data dissemination, including reports, presentations, journal articles, and other publications. The disseminating entity must notify the data providing entity in advance of any dissemination and provide [a mutually agreed upon amount of time] for review. Dissemination without approval by the data providing entity will result in the termination of this Data Sharing Agreement and a ban on all use and dissemination of the data by the disseminating entity. [The data sharing entity may provide and require the use of acknowledgement, disclaimer, and/or explanatory language for disseminations.]

Effective Dates

This Data Sharing Agreement is in effect from [specify: the date signed by both parties or some other date] through [specify: an end date, generally not more than 5 years from the start date].

List of Attachments

[No attachments]

[or]

[Attachment # – title of attachment – number of pages in attachment"]

Approval Signatures

For the Maryland Department of Health and Mental Hygiene, Prevention and Health Promotion Administration, Infectious Disease Bureau:

[name]
Name

[title]
Title

_____
Signature

_____
Date

For [name of other entity]:

[name]
Name

[title]
Title

_____
Signature

_____
Date

Appendix C: HIV Surveillance Program Data Security and Confidentiality Procedures Manual

[each program's Procedures Manual is another appendix]