SOUTH DAKOTA DEPARTMENT OF HEALTH

SOUTH DAKOTA DEPARTMENT OF HEALTH

Division of Disease Prevention and Control Data Security and Confidentiality Manual

Contents

1.0 PROGRAM POLICIES AND RESPONSIBILITIES

This Data Security and Confidentiality Manual has been developed to guide the secure and confidential handling of data across surveillance and program areas related to Human Immunodeficiency Virus (HIV), Ryan White, Sexually Transmitted Infections (STI), Tuberculosis (TB), and other communicable disease (EPI) prevention efforts.

In accordance with South Dakota Codified Law 34-22-12, physicians, hospitals, laboratories, and institutions are legally required to report communicable diseases to the Department of Health (DOH). At the same time, individuals are entitled to privacy protections under the U.S. Constitution, the Public Health Service Act, South Dakota state law, and various DOH administrative policies and procedures.

Relevant policies include:

- **GA-07.1**: *Data Suppression and Release Guidelines* (Issued: Nov. 1, 2006; Revised: July 1, 2025)
- **GA-12**: *HIPAA – General Provisions* (Issued: Nov. 17, 2018; Revised: July 1, 2025)
- **GA-22**: *Public Records Requests* (Issued: Nov. 1, 2006; Revised: July 1, 2024)
- **GA-23**: *Records Management* (Issued: Nov. 1, 2006; Revised: July 1, 2025)
- **GA-32**: *Vital Records Accessibility and Use* (Issued: Nov. 1, 2006; Revised: July 1, 2025)

For further details, please refer to **Appendices C and D**.

National program requirements to protect HIV, viral Hepatitis, STI and TB surveillance data have been established by the Centers for Disease Control and Prevention of the public health services in the United States Department of Health and Human Services (CDC)[1].

[1]*Centers for Disease Control and Prevention (CDC). Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, STD and TB 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.*

1.1 POLICIES AND PROCEDURES

The South Dakota Department of Health (SDDOH or DOH), Division of Disease Prevention and Control (DPC) used the CDC data security and confidentiality guidelines to develop this data security and confidentiality policy manual, which is implemented throughout the programs and diseases and is reviewed annually.

The DPC policies and procedures for data security and confidentiality are covered by this policy manual. All authorized individuals are responsible for completing annual data security and confidentiality training and have access to this policy manual on a shared network drive:
https://doh.sd.gov/topics/diseases/infectious-diseases/data-confidentiality-security/

Only DOH personnel and program contractors who have a need-to-know will have access to disease-specific surveillance data with identifiers. This manual applies to all staff, contractors, fellows, and interns working within DPC. The South Dakota Bureau of Information Database Administrators are also included as a surveillance unit within the policy.

The Program Managers and Epidemiologists are responsible for managing federal grants, case management within South Dakota Electronic Disease Surveillance System (SDEDSS) and HIV/Acquired Immunodeficiency Syndrome (AIDS) Reporting System (eHARS), assigning disease case investigations to the Disease Intervention Specialists (DIS), dissemination of surveillance data, education, and transferring data to CDC. DOH is a

centralized health department so Regional Managers and DIS are located across the state in field office and provide DOH services in the community. The Regional Managers are responsible for supporting case management within SDEDSS and assigning disease case investigations to the DIS. The DIS are responsible for all case investigations, active case finding, case follow-up, and connection, such as linkage to care, for Ryan White services. Informatics staff are responsible for supporting the SDEDSS, dissemination of surveillance data using dashboards, and transferring data to CDC.

1.2 OVERALL RESPONSIBLE PARTY (ORP)

As part of the program requirements, the State Epidemiologist is designated as the ORP for the Division of Disease Prevention and Control. The ORP has the responsibility for the security of the HIV surveillance system (eHARS) and the SDEDSS and will annually certify, using the *Security and Confidentiality Program Requirement Checklist*, that all programs are following the security and confidentiality requirements established by CDC.

1.3 PROGRAM ROLES AND ACCESS CONTROL

SDEDSS is utilized for the surveillance and case management of all communicable diseases. Its security protocols comply with established Health Insurance Portability and Accountability Act (HIPAA) standards. Each user is provided with a unique username and password. User profiles are linked to one or more roles that define their permissions and access levels within various system functionalities.

Additionally, users are associated with specific groups, which govern the events they are authorized to access.

Access to identifiable surveillance information by individuals managing other disease registries (e.g. TB, STI, EPI) will be restricted to users within DDPC, provided their security clearance meets the standards outlined in this document. Only the information essential for delivering public health services or medical care will be disclosed.

Access to client and patient records will be restricted solely to surveillance activities and only granted to individuals authorized by the appropriate program manager, epidemiologist, or ORP.

Only authorized personnel are permitted to:

- Access the information systems (e.g. log into the network, establish connections),
- Execute specific system functions (such as running designated programs or procedures), and
- Create, view, or modify system objects, programs, or configuration parameters.

Refer to *Maven user list* for authorized users.

The Director of Infectious Disease Informatics and/or the Deputy Administrator of Disease Prevention Services (ODPS) Programs are responsible for completing the following tasks:

1. Semi-annually review the SDEDSS audit logs to assess whether unauthorized data access has occurred. Breach of security and confidentiality pertaining to disease surveillance information may result in suspension or termination based on the severity of the offense. Disciplinary actions are determined by the ORP.

2. Authorize group authenticators (administrators, super users, etc.) to have information system access.

3. Manage a list of specific authorized staff (*Maven user list*) that has access to identifiable patient data.

4. Authorize approval for informatics staff to grant or add access to additional users, and review periodically a log documenting authorized viewer.

1.4 ANNUAL TECHNOLOGY REVIEW AND BACKUP/RECOVERY PLAN

An annual review of emerging technologies will be conducted by the Deputy Administrator of ODPS Programs, the Director of Infectious Disease Informatics, and the Bureau of Information and Technology (BIT) point of contact to ensure that data security policies and procedures remain effective. Refer to the Revision Table on page 16 for details.

Each year, the Director of Infectious Disease Informatics and the Deputy Administrator of ODPS Programs will assess the data security policies and procedures to confirm compliance with CDC program requirements, using the *Periodic Assessment Checklist* provided in **Appendix I**.

Whenever changes to information systems security are proposed, the BIT point of contact, Deputy Administrator of ODPS Programs, and Director of Infectious Disease Informatics will collaborate with program managers and epidemiologist to develop appropriate technical solutions. This collaboration is essential to ensure that the security and confidentiality of communicable disease surveillance data are not compromised.

Backup and Recovery Plan:
Backup and Recovery is the combination of manual and machine procedures that can restore lost data in the event of hardware or software failure. Routine backup of databases and logs of computer activity are part of a backup and recovery program. This policy ensures the protection of client data assets from loss due to hardware and software failures or human error.

Backups copy data to provide off-site storage to complement Business Continuity or Disaster Recovery Planning (DRP). Although DRP does incorporate data backup, it also includes alternate hardware, facilities, and telecommunications. Conventional Backup and Recovery, on the other hand, uses the original hardware, facilities, and telecommunications. Under Data Center policy, BIT is responsible for all storage and maintenance of the data.

The SDDOH Continuity of Operations (COOP) plan lists the mission-essential functions for SDDOH. The functions have been prioritized in the event of disruption. This ensure the functions are resumed as quickly as possible. Refer to COOP Plan here.

Backup Information

- **Full Backups:**
  On the 1st day of each month, a complete backup is conducted for all production databases hosted on ADABAS, Oracle, and MS SQL Server. These full backups are retained for 62 days and also archived for 13 months.
- **Differential Backups:**
  Differential database backups—capturing only data changes since the last full backup—are performed daily, except on the 1st day of each month. These differential backups are retained for 62 days.
- **Transaction Log Backups:**
  Hourly transaction log backups are performed for all production databases at the beginning of each hour, unless an alternate schedule has been requested by the database owner. These backups are retained for 62 days.

- **Replication and Off-Site Storage:**
  All backups are replicated between two data centers located in Pierre, SD, ensuring redundancy and data protection.
- **Encryption and Secure Transfer:**
  Each night, drives are backed up on campus and then encrypted and securely transferred to an off-site storage location.

1.5 SECURITY BREACHES

All personnel authorized to access surveillance data are required to report any suspected security breaches. This responsibility also extends to non-surveillance staff, who will receive training that includes this directive. Any suspected breach must be reported immediately to ORP. In cases involving potential electronic data breaches, the BIT must also be notified without delay. The ORP will maintain documentation detailing the investigation, findings, and corrective actions taken. Any breach of confidentiality will be promptly investigated to identify the cause and implement necessary remedies.

If a breach results in the unauthorized disclosure of personal information (i.e., a breach of confidentiality), it must be reported immediately to the ORP. The ORP will then notify the appropriate CDC personnel, including the CDC Program Manager, DHAP, NCHSTP, and HRSA Program Manager. In coordination with legal counsel, the ORP will determine whether the incident requires reporting to law enforcement. Refer to the *Breach Report Form* in Appendix K for further guidance.

To reduce the risk of security breaches involving surveillance data and protected health information (PHI), staff must verify client identity using at least two identifiers, such as name and date of birth.

1.6 ANNUAL SECURITY TRAINING

All individuals with access to communicable disease surveillance data are required to complete annual data security training. This applies to IT personnel, staff with access to servers, workstations, backup devices, and any other systems storing or processing surveillance data. The same training and agreements apply to all such individuals—no job-specific variations are permitted. The date of the initial training must be documented in the employee's personnel file.

The training will address the data security and confidentiality standards outlined in this document, including physical and electronic data security measures, confidentiality protocols, and procedures for data release and sharing. Training materials will include this document, which will be reviewed and updated at least annually or as necessary.

Each member of the surveillance staff and all persons described in this document who are authorized to access case-specific information must be knowledgeable about the SDDOH's Data Security and Confidentiality policies and procedures and will be required to annually perform the *Data Security and Confidentiality Program Requirement Checklis*t. Refer to **Appendix O** for checklist.

Each individual user must sign (electronically or physically) a confidentiality statement on an annual basis. By signing, the employee affirms their understanding and agreement that surveillance data will not be disclosed to any unauthorized individual, party, or entity. The original signed statement will be filed in the employee's personnel file. All subsequent signed statements will be maintained in a working file. Refer to **Appendix B** for *Confidentiality Statement*.

1.7 NEW-HIRE TRAINING

All new hires that will have access to communicable surveillance data must complete the Data Security and Confidentiality training and must sign a confidentiality statement before access to surveillance data is authorized. This signed statement indicates that the employee understands and agrees that surveillance information or data will not be released to any unauthorized individual, party, or other entity. The original statement will be placed in the employee's personnel file and a copy will be maintained in a working file. Refer to **Appendix B** for *Confidentiality Statement.*

1.8 INDIVIDUAL SECURITY RESPONSIBILITIES

Each staff member authorized to access communicable disease surveillance data is responsible for the following:

- **Challenging Unauthorized Access:** Question anyone accessing surveillance data who is not clearly authorized. Authorized users who have completed the required training are listed in the link provided in **Appendix F**.
- **Reporting Breaches:** Immediately report any suspected breach of confidentiality to the State Epidemiologist (ORP). The ORP or their designee will notify the CDC contacts as required.
- **Using Sound Judgment:** Exercise discretion and professionalism in all activities involving surveillance data. If situations arise that aren't addressed by this manual, consult the State Epidemiologist (ORP) or Infectious Disease Informatics Director for guidance.
- **Securing Devices and Access:** Safeguard all devices used to access surveillance data (workstations, laptops, etc.) and protect login credentials such as passwords, keys, and access codes. Avoid infecting systems with viruses and protect hardware from environmental damage (e.g., heat or cold).
- **Maintaining Confidentiality:** Ensure that surveillance data is not visible or audible to unauthorized individuals. Avoid discussing confidential information in shared or public spaces. Prevent unauthorized viewing of paperwork or computer monitors.
- **Limiting Access to Secure Areas:** Ideally, only staff with similar roles and authorization levels should be present in secure areas.
- **Handling Phone Communications:** Answer incoming calls using non-specific identifiers (e.g., "Department of Health" or first name only). Outgoing calls involving confidential information should be conducted privately and securely. Do not leave identifying details on voicemail unless prior arrangements confirm it is secure.
- **Safe Use of Systems:** Do not access SDEDSS while simultaneously browsing the public internet. Be cautious when using applications such as Outlook alongside SDEDSS to prevent inadvertent data transmission. Use secure email settings within Outlook when sending confidential information outside the DOH firewall.

2.0 DATA COLLECTION AND USE

2.1 DATA USE PURPOSE

Public health data are collected to prevent disease and promote health across South Dakota. This information supports:

- Health needs assessments and surveillance,
- Public health policy development,
- Emergency preparedness and response, and
- Program evaluation and improvement.

2.2 MINIMUM DATA

Only the minimum data necessary to achieve public health objectives is collected, as outlined in the manual. Refer to: M:\DOH\Disease Prevention\ODP\EPI Manual\Policies.

2.3 PERSONAL IDENTIFYING INFORMATION (PII)

PII is collected strictly when needed for disease prevention or investigation. De-identified data is used for analysis and reporting to maintain confidentiality.

2.4 PUBLIC HEALTH RESEARCH

Access to named surveillance data for research purposes requires:

- Demonstrated need for identifiable data,
- Institutional Review Board (IRB) approval,
- A signed confidentiality agreement specifying access terms and data handling.

Use of de-identified data may also require IRB approval depending on the nature and quantity of data requested. All research-related data access must be reviewed and approved by the ORP.

3.0 DATA SHARING AND RELEASE

3.1 ORP APPROVAL

Sharing confidential surveillance data outside the surveillance unit requires:

- A clear public health justification,
- Assurance that surveillance activities are not hindered,
- Protection of public trust in the surveillance system, and
- Prior approval from the ORP.

3.2 RISK & BENEFIT ASSESSMENT

If a data-sharing request involves identifiable information and is not addressed by existing policies, the ORP must evaluate the potential risks and benefits before granting access.

3.3 PROGRAM-SPECIFIC DATA SECURITY

Access to surveillance data by external disease programs is limited. The ORP ensures:

- Justification of access,
- Risk/benefit analysis,
- Adequate security settings in SDEDSS.

Offsite access for on-call staff is granted annually and must follow all established security protocols.

3.4 RELEASE OF PUBLIC HEALTH INFORMATION

Access to communicable disease information or data for non-public health purposes, such as litigation, discovery, or court order, will be granted only to the extent required by law.

Release of any data or information with identifiers (confidential information) will be in accordance with SDCL 34-22-12.1.

34-22-12-1. Confidentiality of reports—Exceptions. Any report required to be submitted pursuant to § 34-22-12 is strictly confidential medical information. No report may be released, shared with any agency or institution, or made public, upon subpoena, search warrant, discovery proceedings, or otherwise. No report is admissible as evidence in any action of any kind in any court or before any tribunal, board, agency, or person. However, the

Department of Health may release medical or epidemiological information under any of the following circumstances:

1. *For statistical purposes in such a manner that no person can be identified;*

2. *With the written consent of the person identified in the information released;*

3. *To the extent necessary to enforce the provisions of this chapter and rules promulgated pursuant to this chapter concerning the prevention, treatment, control, and investigation of communicable diseases;*

4. *To the extent necessary to protect the health or life of a named person;*

5. *To the extent necessary to comply with a proper judicial order requiring release of human immunodeficiency virus test results and related information to a prosecutor for an investigation of violation of §22-18-31 and*

6. *To the attorney general or an appropriate state's attorney if the Secretary of the Department of Health has reasonable cause to suspect that a person violated §22-18-31.*

3.5 DATA REQUEST NOT COVERED BY EXISTING DATA-RELEASE POLICY

Requests not explicitly addressed by existing data release policies must also follow **SDCL 34-22-12.1**. Identifiable information may not be released without ORP approval. Even requests for de-identified data may require ORP review, depending on the volume and type of data.

3.6 DISSEMINATION OF DATA

Data is regularly shared with community partners to raise awareness of disease trends in South Dakota. Each program manager or epidemiologist publishes annual statistics, and the HIV Program Manager contributes to the Epidemiological Profile, updated every 4–5 years.

3.7 DATA QUALITY

SDEDSS undergoes continuous validation and annual clean-up prior to data submission to CDC. Co-morbidities and disease links (e.g., STI and HIV) are tracked for authorized users including but not limited to DIS, program managers, and epidemiologists.

For example, STI and HIV surveillance efforts share data to support investigations and identify additional HIV cases. DIS staff play a key role in identifying contacts and resolving "No Identified Risk" (NIR) cases. Vital Records in collaboration with HIV Program Manager conduct death certificate review on a biannual basis.

3.8 DATA RELEASE POLICY

All data releases must comply with SDDOH Administrative Policy and Procedure GA-7.1 and be approved by the ORP. Refer to **Appendix D**.

4.0 PHYSICAL SECURITY

4.1 HANDLING SURVEILLANCE INFORMATION AND PII

Security Protocols for Handling Surveillance Information

All paper copies of surveillance data containing personally identifiable information (PII) must be stored in locked filing cabinets located within a secured, locked room.

When PII is removed from the secured area—for example, in supporting notes or other hard-copy formats—documents must include only the minimum information necessary to complete the task. When feasible, terms should be coded to obscure any direct association with a specific disease.

- Examples of disease coding:
    - HIV- 900
    - AIDS- 950
    - Syphilis- 700
    - Gonorrhea- 300
    - Chlamydia- 200

Remote Access During Business Travel

When accessing SDEDSS while traveling for work, staff must:

- Use a State-owned, BIT-supported device.
- Access SDEDSS only from a secure, private room.
- Use secure access methods such as Citrix, a State VPN, My Apps, or an approved SDEDSS secure portal to ensure data encryption.
- Log off SDEDSS and/or Citrix/VPN and lock the computer when not in the room.
- Avoid using unsecured or public internet connections (e.g., networks with weak or no passwords).
- Use a State-supported device hotspot when possible.
- Complete the *Authorization for Offsite Access to SDEDSS* form included as **Appendix N** before accessing the system from any offsite location.

Field or Home Use of Surveillance Information

When PII—whether in hard copy or digital form—is taken into the field or to a private residence, staff must follow all established security standards.

If business travel prevents the return of PII to the secured area by the end of the business day, prior approval must be obtained from the appropriate program manager or epidemiologist. In general, surveillance information must not be taken to private residences unless necessary.

In rare and exceptional situations, such as a sudden weather emergency, surveillance data may be taken home without prior approval if returning to the office is unsafe or impossible. In such cases:

- The staff member must notify (or attempt to notify) their supervisor.
- Extra precautions must be taken at home to protect the data.
- Paper case report forms (completed or in progress) must be transported in a locked satchel or briefcase.

Home Access to SDEDSS

When working from home:

- Staff must use a State-owned, BIT-supported device.
- Secure access must be maintained through the Citrix application or an approved SDEDSS portal.
- Use of SDEDSS must occur in a designated, secure, private room.
- The computer must be locked, and users must log off SDEDSS and/or Citrix when not present in the room.
- Unsecured or public internet connections must not be used.
- When possible, access SDEDSS via a State-supported device hotspot.

- The *Authorization for Offsite Access to SDEDSS* form must be completed in advance. Refer to **Appendix N**.

4.2 CROSSCUTTING OF CONFIDENTIAL DOCUMENTS

All confidential paper documents must be shredded using commercial-grade, crosscutting shredders before disposal.

4.3 INCOMING/OUTGOING MAIL; LONG-TERM PAPER STORAGE AND DATA RETENTION

All incoming mail is sorted by a DOH Secretary. This person is required to sign the department confidentiality statement. The mail is then dispersed to the respective employee. If the employee is out of the office, the mail is stored in a secure environment, until the return of the employee.

No outgoing envelopes have any direct or indirect reference to the specific disease, such as HIV/AIDS.

HIV/AIDS Only: Senders of confidential information are instructed to address mail to the corresponding program manager. Whenever confidential information is mailed, double envelopes must be used, clearly marked "Confidential". All outgoing mail containing patient identifiers is marked "Confidential", double enveloped, and sent "Return Service Requested".

In 1967, the South Dakota Legislature established the Records Management Program and the Records Destruction Board. In the same act, the Legislature required every State agency to develop a records retention and destruction schedule. The DOH retention and destruction policies, DOH 78 – DOH 106 can be found on pages 73-87 in the Department Of Health Records Retention and Destruction Schedule Manual which is located at: https://boa.sd.gov/central-services/records-management-stateretentionmanuals.aspx

Secure Areas

All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must be within a secure locked area.

Cubicle walls with additional soundproofing can be used. When cubicles are part of the office structure, cubicles where sensitive information is viewed, discussed, or is otherwise present should be separated from cubicles where staff without access to this information is located.

It can be considered in areas where phone calls can possibly be overheard to use headsets.

Rooms containing surveillance data must not be easily accessible by window. Window access is defined as having a window that could allow easy entry into a room containing surveillance data. This does not mean that the room cannot have windows; rather, windows need to be secure. If windows cannot be made secure, surveillance data must be moved to a secure location to meet this requirement.

A window with access, for example, may be one that opens and is on the first floor. To secure such a window, a permanent seal or a security alarm may be installed on the window itself.

4.4 HANDLING OF PII DOCUMENTS

All surveillance data information with identifiers is secured in locked filing cabinets stored in a locked room when surveillance personnel are not present. Cleaning and maintenance personnel do not have access into locked files.

Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP.

4.5 LINE LISTS

Line-lists typically contain the client's name, Date of Birth (DOB), status, and risk information. Line lists of clients will not be printed or mailed without prior approval from the corresponding program manager. Line lists will be de-identified with numeric ID to neither directly nor indirectly identity the contents of the line-list. Transmission between the printer and the personal computer are encrypted.

Only client information necessary for daily work is transported into the field.

When identifying information is taken from secured areas and included on a line-lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and where possible must be coded to disguise any information that could easily be associated with STI, HIV or AIDS.

The requirement applies to information or data taken from secure areas.
It does not refer to data collected from the field and taken to secure areas. While coding of terms is encouraged, there may be occasions when it cannot be done, for example, when uncoded terminology must be abstracted from a medical chart on a HIV NIR case during an investigation.

5.0 ELECTRONIC DATA SECURITY

5.1 ELECTRONIC PROTECTIVE SOFTWARE

Maximum security practice dictates that communicable surveillance data be maintained in a manner where layers of security protections can be provided, such as on-premises file servers maintained by BIT or the state's Microsoft Azure cloud tenant.

Remote sites that are within the firewall, such as Department of Health DIS field offices, access the central surveillance server for authorized surveillance activities through a secured method as required by the DOH (e.g. encryption). For remote sites that are outside the firewall an additional level of security exists incorporating the use of AES standards approved by the respective ORP. A BIT supported Citrix solution including but not limited to VPN and MS Office 365 guest accounts, requires users to login to gain access to the State's internal network, ensuring continuity of critical DOH function. Physical access to the central surveillance server for authorized surveillance activities on and off-site are handled through a secured method as required by the DOH.

The LAN server is housed in a locked room accessible only to computer systems administrators. eHARS is protected by a password security system and is accessible only to the surveillance coordinator or their designee. SDEDSS security standards comply with established HIPAA requirements. Each user is assigned a unique username and password. SDEDSS operates within a role-based security environment, ensuring users can only view the data they are authorized to access. Login authentication for SDEDSS utilizes both password-based and

Single Sign-On (SSO) authentication methods, where password hashes are compared against the hashed (SHA) passwords stored in the database. SDEDSS also captures detailed information for each login attempt, including the username, timestamp, server source IP address, and browser user-agent.

5.2 APPROVAL BY ORP FOR ELECTRONIC DATA TRANSFER

All data collection methods and data transfers must be approved by the ORP and must include access controls. Any confidential surveillance data must be encrypted prior to electronic transmission. Similarly, any ancillary databases or electronic files used for surveillance purposes must also be encrypted when not actively in use.

Electronic files intended for use by authorized surveillance personnel should remain encrypted until accessed. If these files are accessed outside of a secure area, they must be protected with real-time encryption or an equivalent security measure.

This encryption requirement also applies to surveillance data received electronically from external sources such as clinical data management systems or laboratories. Data extracts from these sources must be treated with the same level of security as extracts from the primary surveillance database.

For interstate data sharing (Interstate Notification), data transfers must comply with National Institute of Standards and Technology (NIST) guidelines.

When transferring case-specific information between the HIV Surveillance Coordinator and the DIS, communication should be conducted via telephone, standard mail, or email that substitutes the terms HIV or AIDS with the corresponding 900/950 codes or uses SDEDSS terminology. Use of fax machines for this purpose is strongly discouraged.

In rare cases where faxing is unavoidable, the sender must contact the recipient beforehand to ensure they are present to receive the fax immediately. This is essential to prevent unauthorized access to sensitive information.

Please refer to **Appendix H** for additional details.

5.3 ENCRYPTION ELECTRONIC DATA

When electronically transmitting case-specific information, any transmission that does not use an encryption tool compliant with the Advanced Encryption Standard (AES) and approved by the ORP must not include identifying details or language that could be linked to a specific disease. Terms such as HIV, AIDS, STI, TB, or any other recognizable disease name or behavioral descriptor must not appear anywhere in the communication, this includes the message content as well as sender or recipient names and labels.

The purpose of this guideline is to prevent third parties from identifying individuals as part of a disease risk group. For example, when locating an individual with HIV during a "No Identified Risk" (NIR) investigation, you must avoid sending letters, leaving business cards, or voice messages at the person’s home that contain any references that could suggest an HIV or AIDS connection.

Likewise, if a third party contacts the number provided on a letter or card, the phone greeting must not reveal that the call is being received by an HIV/AIDS surveillance unit or any other disease-specific program.

If secure fax or encrypted email is used, though the CDC advises against these methods, great care must be taken to avoid linking any disease or risk factor with identifiable personal information. Instead of using disease

names, you must use corresponding disease codes (e.g., 900, 950, 200/300, 700), where such codes are assigned.

Per CDC policy, any moderately or highly sensitive information, or data considered limited access or proprietary, must be encrypted before being transmitted to or from CDC, whether electronically or physically. All such transmissions must use AES encryption. Refer to **Appendix G** for more details.

Currently, CDC requires this category of electronic data to be transmitted via its Secure Access Management Services (SAMS) portal, which uses Secure Sockets Layer (SSL) technology to establish a secure, encrypted connection for data transmission.

5.4 LAPTOPS AND PORTABLE DEVICES

Laptops, tablets, cell phones, and other portable devices that access or store surveillance data containing personal identifiers must use encryption software. However, storing such data on external storage devices or removable hard drives is strongly discouraged.

When surveillance data with identifiers must be stored on an external device or a laptop's removable hard drive, the data must be encrypted. These storage devices must be physically separated from the laptop and securely stored when not in use. The decryption key must not be stored on the laptop itself. Portable devices that do not support external or removable storage must utilize encryption software that complies with federal standards. Laptops or other devices that handle STI or HIV surveillance data must connect through a secure wireless network.

All removable or external storage devices containing surveillance data with personal identifiers must adhere to the following requirements:

1. Only the minimum necessary information, as determined by the Deputy Administrator of ODPS Programs, should be stored to complete assigned tasks.
2. Devices must be encrypted or securely locked away when not in use.
3. Except for devices designated for data backups, all devices should be properly sanitized immediately after the completion of their task.
4. External storage devices include, but are not limited to, USB flash drives (memory sticks) and removable hard drives.

5.5 DESTRUCTION OF INFORMATION ON HARD COPIES AND ELECTRONIC DEVICES

Data on physical or digital storage media must be securely destroyed before disposal or reuse:

- Acceptable methods include overwriting, degaussing, or physical destruction (including the device casing).

For surplus machines, request a 3-pass hard drive wipe via the BIT Help Desk.

ANNUAL REVIEW AND REVISION HISTORY

Date	*Action*	*Section*	*Reviewer*
10/22/25	*Updated/Revised*	*Entire document*	*State Epidemiologist, Josh Clayton; Deputy Administrator of ODPS Programs, London Zerfas; Informatics Surveillance lead, BIT, Daniel Hoblick*
10/31/2022	*Updated/Revised*	*1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.8, 1.9, 2.2, 2.4, 3.1, 3.2, 3.3, 3.7, 4.1, 4.2, 5.1* *Appendix A-Q*	*State Epidemiologist, Josh Clayton; HIV Program manager, Sarah Zaiser; Infectious Disease Director, Angela Cascio; Informatics Surveillance lead, John Shmulsky; BIT, Daniel Hoblick,*
8/24/2021	*Updated/Revised* *Updated*	*1.1, 1.2, 1.4, 1.8, 4.0, 4.1* *Appendix A, B, E, F, O*	*Informatics Surveillance Lead, John Shmulsky, HIV Program Manager, Susan Gannon; BIT, Roger Reed, Megan Lehmkuhl*
5/2/2019	*Updated/revised* *Revised* *Revised* *Updated*	*1.0, 1st paragraph; 1.1, 2nd and 3rd paragraph; 1.4, Backup information, 6th paragraph; 1.8 (9)* *3.7, 4th paragraph* *4.1, 2nd and 6th paragraph* *Appendix A, C, D, E, F, I, J, O*	*Surveillance Program Manager, Nick Hill, Data Manager, Eric Grimm, BIT, Mark Zickrick, HIV Program Manager Susan Gannon*
6/21/2018	*Added* *Updated* *Updated* *Updated*	*3.3, 2nd paragraph* *Appendix A* *Appendix E* *Appendix F*	*Surveillance Program Manager, Nick Hill, BIT Mark Zickrick, HIV Program Manager, Susan Gannon*
7/21/2017	*Revised* *Page 4* *Amended policy from ODP to ODPS* *Updated*	 *1.1* *All* *Appendix* *D, E, F, J, N*	*Surveillance Program Manager, Nick Hill, BIT, Mark Zickrick, HIV Surveillance Program Manager, Susan Gannon*
10/17/2016	*Revised* *Page 13* *Page 20* *Page 23* *Page 35* *Requirement Check List* *Requirement Check List*	 *4.1* *Appendix A* *Requirement 5.5* *Appendix E* *Requirement 29* *Requirement 30*	*Nicholas Hill Surveillance Program Manager* *Mark Zickrick BIT* *Christine Olson HIV Surveillance Program Manager*

08/21/2015	*Revised* *1.4 Page 5* *5.1 Page 16* *5.4 Page 18* *5.5 Page 19* *Appendix F Page 34* *Added Appendix N Page 60* *Appendix O* *Page 59 (Requirement 33, 34, & 35)*	*Entire Document*	*Nicholas Hill Surveillance Program Manager* *Mark Zickrick BIT* *Christine Olson HIV Surveillance Program Manager*
05/15/2015	*Added updated 35 Requirement Pages*	*Appendix B-2*	*HIV Surveillance Program Manager*
04/15/2015	*Added CDC Validation Letter*	*Appendix M*	*HIV Surveillance Program Manager*
11/04/2014	*Updated Contacts*	*Appendix E*	*HIV Surveillance Program Manager*
02/10/2014	*CDC Revisions*	*(1.6) (3.4) (4.1) (4.6)*	*HIV Surveillance Program Manager*
08/13/2013	*Amend policy to make it applicable to the entire ODP*	*All*	*HIV Surveillance Program Manager*
04/19/2012	*Update Table 1 Data System Access Role*	*Table 1*	*HIV Surveillance Program Manager*
02/24/2011	*Included Signature of ORP and ODP Administrator*	*Page 19*	*HIV Surveillance Program Manager*
02/23/2011	*Update Table 1 Data System Access Role*	*Table 1*	*HIV Surveillance Program Manager*
07/01/2010	*Update Table 1 Data System Access Role*	*Table 1*	*HIV Surveillance Program Manager*
07/06/2009	*Corrected Spelling Error*	*Procedures*	*HIV Surveillance Program Manager*
07/01/2009	*Update Table 1 Data System Access Role*	*Table I*	*HIV Surveillance Program Manager*
07/01/2008	*Update Table 1 Data System Access Role*	*Table 1*	*HIV Surveillance Program Manager*
07/01/2007	*No Changes*	*Reviewed Document t*	*HIV Surveillance Program Manager*
05/06/2006	*This is a new policy*	*N/A*	*HIV Surveillance Program Manager*

APPENDIX A – CERTIFICATION OF COMPLIANCE

CERTIFICATION OF COMPLIANCE WITH THE NCHHSTP DATA SECURITY AND CONFIDENTIALITY STANDARDS AND DESIGNATION OF OVERALL RESPONSIBLE PARTY (ORP)

We certify our program complies with the National Center for HIV/AIDS, Viral Hepatitis, STD and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs (2011) available at:
https://www.cdc.gov/sti/media/pdfs/PCSIDataSecurityGuidelines.pdf

We acknowledge that all standards in the NCHHSTP Data Security and Confidentiality Guidelines are implemented for the HIV surveillance and HIV prevention programs funded by **NOFO PS24-0047** and for programs with which we share data, unless otherwise justified in an attachment to this statement. We agree to ensure that all standards are applied to all local/state staff and sub-recipients that have access to and/or maintain confidential, personally identifiable public health data. We agree to ensure that all sites where applicable public health data are maintained are informed about the standards. Documentation of required local data policies and procedures is on file with the Overall Responsible Party (ORP) and available upon request.

The signed Certification of Compliance statement by the designated ORP will cover the duration of the PS24-0047 or when changes in the ORP designation occur.

Please select one of the options below:

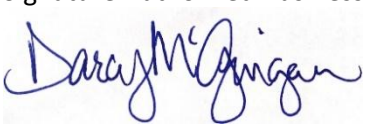
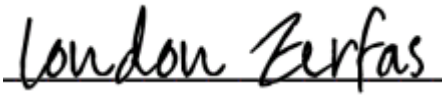
☒ In full compliance with the Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs (2011) for HIV surveillance and HIV prevention programs funded by **NOFO PS24-0047**. We ensure that all standards are applied to all local/state staff and sub-recipients that have access to and/or maintain confidential, personally identifiable public health data. We ensure that all sites where applicable public health data are maintained are informed about the standards; there are no attachments to this statement.

☐ Not in full compliance with the Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs (2011). We are pursuing compliance for HIV surveillance and/or HIV prevention programs funded by **NOFO PS24-0047**. A justification for non-compliance is included as an attachment.

Instructions for Justification Statement: Please describe the reasons for non-compliance with the NCHHSTP Guidelines. Outline the steps being taken to address issues and achieve full compliance. Include a timeline and provide specific information for program areas that are non-compliant or pursuing compliance (e.g., surveillance, prevention, information technology, sub-recipients, community-based organizations, programs with which you share data etc.).

Name(s), title, and organizational affiliation of the proposed ORP(s)

ORP Name	Title	Affiliation
Josh Clayton	State Epidemiologist	South Dakota Department of Health, Division of Disease Prevention and Control

Applicant/Jurisdiction Name South Dakota Department of Health	Grant/Cooperative Agreement Number NU62PS924825
Signature Overall Responsible Party (ORP) 	Date 12/5/25
Signature Authorized Business Official 	Date 12/5/25
Signature Principal Investigator (s) 	Date 12/5/25

APPENDIX B – CONFIDENTIALITY OATH

All Department of Health, Division of Disease Prevention and Control, personnel including career service, exempt, contractors, and interns who have access to confidential medical or epidemiological information must be knowledgeable of SD Codified Laws 34-22-12, 34-22-12.1, 34-22-12.2, 22-18-31, and SD Department of Health Administrative Policies and Procedures, Statement No. GA-07.1, GA-12, GA-22, GA-23, GA-32, and Data Security and Confidentiality Guidelines.

I acknowledge the following:

1. I have read and received a copy of SDCL 34-22-12.1, SDCL 34-22-12.2, and SD Department of Health, Administrative Policies and Procedures, Statement GA-07.1, GA-12, GA-22, GA-23, and GA-32.
2. Release of any data or information with identifiers (confidential information) will be in accordance with SDCL 34-22-12.1.
3. Any confidential information to be disposed of will be shredded.
4. All confidential information, on paper or other storage media, will be kept in a locked file cabinet when not being used.
5. All confidential information that I am working with will be locked up when I leave my workstation unattended or receive unauthorized visitors at my workstation.
6. I will conduct telephone conversations requiring the discussion of identifiers in my work area or other confidential area only.
7. When working with confidential information on a computer, I will log off when I am finished to prevent unauthorized access to that information.
8. I will not disclose my computer passwords or lend my file or office keys to unauthorized persons.
9. The confidential information generated and used while employed by the State of South Dakota is the property of the State of South Dakota and may not be reproduced or shared without approval of the ORP.
10. I will only discuss identifying information as necessary for my job responsibilities and will ensure that such conversations do not take place in public spaces, including hallways, elevators, restrooms, lunchrooms, or other common areas.
11. Violation of this Confidentiality Oath may result in termination of my employment and/or legal penalties. Legal penalties may apply even after termination of my employment.
12. Authorized personnel who work with identifiable surveillance information will be provided with a copy of the Data Security and Confidentiality Guidelines. I have read and understood the contents of this document and have had the opportunity to ask questions or seek clarification about how it relates to my authorized use of data and information in my role.
13. I will report activities by any individual or entity that I suspect may compromise the confidentiality, integrity or availability of confidential information.

_____/_____/_____

Employee, Independent Contractor, or Intern Signature Print Name Date

I hereby certify that the above person received copies of the pertinent statutes and policy described above.

_____ _____

State Epidemiologist Date

Overall Responsible Party (ORP) (Revised October 2025)

APPENDIX C – SOUTH DAKOTA CODIFIED LAW

22-18-31. Intentional exposure to HIV infection a felony. Any person who, knowing himself or herself to be infected with HIV, intentionally exposes another person to infection by: Engaging in sexual intercourse or other intimate physical contact with another person; Transferring, donating, or providing blood, tissue, semen, organs, or other potentially infectious body fluids or parts for transfusion, transplantation, insemination, or other administration to another in any manner that presents a significant risk of HIV transmission; Dispensing, delivering, exchanging, selling, or in any other way transferring to another person any nonsterile intravenous or intramuscular drug paraphernalia that has been contaminated by himself or herself or Throwing, smearing, or otherwise causing blood or semen, to come in contact with another person for the purpose of exposing that person to HIV infection; is guilty of criminal exposure to HIV.
Criminal exposure to HIV is a Class 3 felony.

34-22-12. Mandatory communicable disease reports from physicians, laboratories, and institutions- - Surveillance and control - - Adoption of rules. The State Department of Health shall provide for the collection and processing of mandatory reports of identifiable and suspected cases of communicable disease, communicable disease carriers, and laboratory tests for communicable disease carriers, from all physicians, hospitals, laboratories, and institutions. The State Department of Health shall maintain a complete case register of tuberculosis suspects, active and presumably active cases, tuberculosis contracts, and arrested or presumably arrested cases. The State Department of Health shall provide information necessary for disease surveillance and control. To implement this section, the State Department of Health may adopt, pursuant to chapter 1-26, rules specifying the methods by which disease reports shall be made, the contents and timeliness of such reports, and diseases which shall be considered in such reports.

34-22-12.1. Confidentiality of reports- - Exceptions. Any report required to be submitted pursuant to § 34-22-12 is strictly confidential medical information. No report may be released, shared with any agency or institution, or made public, upon subpoena, search warrant, discovery proceedings, or otherwise. No report is admissible as evidence in any action of any kind in any court or before any tribunal, board, agency, or person. However, the Department of Health may release medical or epidemiological information under any of the following circumstances: For statistical purposes in such a manner that no person can be identified; With the written consent of the person identified in the information released; To the extent necessary to enforce the provisions of this chapter and rules promulgated pursuant to this chapter concerning the prevention, treatment, control, and investigation of communicable diseases; To the extent necessary to protect the health or life of a names person; To the extent necessary to comply with a proper judicial order requiring release of human immunodeficiency virus test results and related information to a prosecutor for an investigation of a violation of § 22-18-31 and to the attorney general or an appropriate state's attorney if the secretary of the Department of Health has reasonable cause to suspect that a person violated § 22-18-31.

Violation of confidentiality as misdemeanor. Except as provided in § 34-22-12.1, any person responsible for recording, reporting, or maintaining medical reports required to be submitted pursuant to § 34-22-12 who knowingly or intentionally discloses or fails to protect medical reports declared to be confidential under § 34-22-12.1, or who compels another person to disclose such medical reports, is guilty of a Class 1 misdemeanor.

APPENDIX D – SDDOH ADMINISTRATIVE POLICIES AND PROCEDURES

Refer to intranet for SDDOH Administrative Policies and Procedures located here.

APPENDIX E – SDDOH DIVISION OF DISEASE PREVENTION AND CONTROL STAFF DIRECTORY

A directory including addresses, phone numbers, and email addresses of DPC staff, including Program Managers, DIS, Regional Managers can be viewed here

APPENDIX F – TABLE OF DATA SYSTEMS ACCESS OVERVIEW: ACTIVE USERS

Active and Inactive users located here.

APPENDIX G – FEDERAL ENCRYPTION STANDARDS

CDC Policy
Encryption is required when any moderately or highly sensitive files, any moderately or highly critical information, or any limited access/proprietary information is to be transmitted either electronically or physically.

Federal Standards
The National Institute of Standards and Technology (NIST) uses the Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197. This standard specifies Rijndael as a FIPS-approved symmetric encryption algorithm that may be used by U.S. government organizations (and others) to protect sensitive information. Federal agencies should also refer to guidance from the Office of Management and Budget (OMB).

Advances Encryption Standard (AES)

Federal Information Processing Standards (FIPS) Publication 197

Published: November 26, 2001; Updated: May 9, 2023

Name of Standard: Advanced Encryption Standard (AES) (FIPS PUB 197).
Category of Standard: Computer Security Standard, Cryptography.
Explanation: To ensure the confidentiality and integrity of sensitive public health data, all electronic data encryption must comply with FIPS 197, the Federal Information Processing Standard that defines the Advanced Encryption Standard (AES). AES is a symmetric block cipher that encrypts data in 128-bit blocks using 128-, 192-, or 256-bit keys. Recognized for its strong security and efficiency, AES is the federally approved standard for protecting sensitive but unclassified information. Under FIPS 197, AES encryption is required for storing or transmitting personally identifiable information (PII) or protected health information (PHI), particularly when such data is shared outside of secure environments. The use of FIPS 197-compliant encryption ensures alignment with HIPAA, CDC data security guidelines, and other federal mandates for safeguarding health surveillance information.
Approving Authority: Secretary of Commerce.
Maintenance Agency: Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).
Reference: https://doi.org/10.6028/NIST.FIPS.197-upd1

APPENDIX H – GUIDELINES FOR THE USE OF FACSIMILE MACHINES

The facsimile machine must be located in a secured, locked room with restricted access. When transmitting confidential information via fax, staff must ensure that identifiable personal information is not associated with specific diseases or risk factors. Disease codes must be used in place of disease names or abbreviations whenever feasible.

Exceptions:

- **TB Control Program** records may include disease names and risk factor information but may only be faxed to licensed medical providers or authorized public health agencies at the state, city, or county level.
- **General Epidemiology Program** records may also include disease names and risk factors when faxed, but only to state, city, or county health departments.

The fax machine located within the DOH is housed in a secure building, inside a lockable room, with limited access for authorized personnel. Designated staff inboxes are available for incoming faxes.

To reduce the likelihood of misdialing or using outdated fax numbers, staff should utilize pre-programmed fax destinations where possible. These numbers must be reviewed periodically to confirm accuracy. When entering fax numbers manually, staff must double-check the number before transmission. Facilities receiving regular faxes should be reminded to notify the DOH of any changes to their fax numbers.

All staff are trained on faxing protocols. A printed reminder outlining proper procedures is posted adjacent to the fax machine. A cover sheet must accompany each outgoing fax and must include the contact information of both the sender and the recipient, as well as the standard confidentiality statement.

APPENDIX I – PERIODIC ASSESSMENT CHECKLIST

For the answer to be "yes" to a question with multiple parts, all boxes must be checked. For each "No" response, provide additional information describing how the program intends to achieve compliance with that standard.

Name of Program being assessed _____

Name of person assessing the program _____

Date: _____

1.0 PROGRAM POLICIES AND RESPONSIBILITES

STANDARD 1.1

In your program, how are staff members who are authorized to access HIV/VH/STI/TB/EPI/BT/Immunization information or data made aware of their data confidentiality and security responsibilities?

_____

_____

Are the following points addressed in your policies and agreements?

☐ Yes ☐ No	Are staff provided training on security policies and procedures and where to find resources?
☐ Yes ☐ No	Does the program have written data security and confidentiality policies and procedures?
☐ Yes ☐ No	Are written policies and procedures reviewed at least annually and revised as needed?
☐ Yes ☐ No	Are data security policies readily accessible to all staff members who have access to confidential, individual-level data? Where are the policies located?_____

STANDARD 1.2

☐ Yes ☐ No	In your program, is there a policy that assigns responsibilities and designates an ORP for the security of the data that is stored in various data systems?
☐ Yes ☐ No	Does the ORP have sufficient authority to make modifications to policies and procedures and ensure that the standards are met?

STANDARD 1.3

☐ Yes ☐ No	Does your program have a policy that defines the roles and access level for all persons with authorized access?

☐ Yes ☐ No	Does your program have a policy that describes which standard procedures or methods will be used when accessing HIV/VH/STI/TB/EPI/BT/Immunization information or other personally identifiable data?

STANDARD 1.4

☐ Yes ☐ No	Does the program have a written policy that describes the methods for ongoing review of technological aspects of security practices to ensure that data remain secure in light of evolving technologies?

STANDARD 1.5

☐ Yes ☐ No	Are written procedures in place to respond to breaches in procedures and breaches in confidentiality? Where are those procedures stored?_____
☐ Yes ☐ No	Is the chain of communication and notification of appropriate individuals outlined in the data policy?
☐ Yes ☐ No	Are all breaches of protocol or procedures, regardless of whether personal information was released, investigated immediately to determine causes and implement remedies?
☐ Yes ☐ No	Are all breaches of confidentiality (i.e., a security infraction that results in the release of private information with or without harm to one or more persons) reported immediately to the ORP?
☐ Yes ☐ No	Do procedures include a mechanism for consulting with appropriate legal counsel to determine whether a breach warrants a report to law enforcement agencies?
☐ Yes ☐ No	If warranted, are law enforcement agencies contacted when a breach occurs?

STANDARD 1.6

☐ Yes ☐ No	Are staff trained on the program's definitions of breaches in procedures and breaches in confidentiality?
☐ Yes ☐ No	Are staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?
☐ Yes ☐ No	Are staff trained on policies and procedures that describe how staff can protect program software from computer viruses and computer hardware from damage due to extreme heat or cold?
☐ Yes ☐ No	Have all persons authorized to access individual-level information been trained on the organization's information security policies and procedures?

☐ Yes ☐ No	Is every staff member, information technology (IT) staff member, and contractor who may need access to individual-level information or data required to attend security training annually?
☐ Yes ☐ No	Is the date of the training or test documented in the employee's personnel file?

STANDARD 1.7

☐ Yes ☐ No	Do all authorized staff members in your program sign a confidentiality agreement annually?
☐ Yes ☐ No	Do all newly hired staff members sign a confidentiality agreement before they are given authorization to access individual-level information and data?

STANDARD 1.8

☐ Yes ☐ No	Do policies state that staff are personally responsible for protecting their own computer workstation, laptop computer, or other devices associated with confidential public health information or data?
☐ Yes ☐ No	Are staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?

STANDARD 1.9

☐ Yes ☐ No	Does your program certify annually that all program standards are met?

2.0 DATA COLLECTION AND USE

STANDARD 2.1

☐ Yes ☐ No	When public health data are shared or used, are the intended public health purposes and limits of how the data will be used adequately described?

STANDARD 2.2

☐ Yes ☐ No	When data are collected or shared, do they contain only the minimum information necessary to achieve the stated public health purpose?

STANDARD 2.3

☐ Yes ☐ No	Does your program explore alternatives to using identifiable data before sharing data, such as using anonymized or coded data? What alternatives are currently in use in your program?_____

STANDARD 2.4

☐ Yes ☐ No	Does your program have procedures in place to determine whether a proposed use of identifiable public health data constitutes research requiring IRB review?

3.0 DATA SHARING AND RELEASE

STANDARD 3.1

☐ Yes ☐ No

In your program, is access to HIV/VH/STI/TB/EPI/BT/Immunization information and data for any purposes unrelated to public health (e.g., litigation, discovery, or court order) only granted to the extend required by law?

What non-public health use of the data are required or allowed by law?

_____

STANDARD 3.2

☐ Yes ☐ No

When a proposed sharing of identifiable data is not covered by existing policies, does your program assess risks and benefits before making a decision to share data?

How are these risks assessed?_____

_____

STANDARD 3.3

☐ Yes ☐ No

When sharing personally identifiable HIV/VH/STI/TB/EPI/BT/Immunization information and/or data with other public health programs (i.e., those programs outside the primary program responsible for collecting and storing the data), is access to this information and/or data limited to those for whom the ORP:

_____

☐ has weighed the benefits and risks of allowing access; and

_____

☐ can verify that the level of security established is equivalent to these standards?

STANDARD 3.4

☐ Yes ☐ No

Is access to confidential HIV/VH/STI/TB/EPI/BT/Immunization information and data by personnel outside the HIV/VH/STI/TB/EPI/BT/Immunization programs:

☐ limited to those authorized based on an expressed and justifiable public health need?; and

_____

☐ arranged in a manner that does not compromise or impede public health activities?; and

_____

☐ carefully managed so as to not affect the public perception of confidentiality of the public health data collection activity and approved by the ORP?

☐ Yes ☐ No

Before allowing access to any HIV/VH/STI/TB/EPI/BT/Immunization data or information containing names for research or other purposes (e.g., for other than routine prevention program purposes), does your program require that the requester:

☐ demonstrate need for the names?; and

_____

☐ obtain institutional review board (IRB) approval (if it has been

determined to be necessary)?; and

☐ sign a confidentiality agreement?

STANDARD 3.5

☐ Yes ☐ No	Does your program have written procedures to review data releases that are not covered under the standing data release policy?
☐ Yes ☐ No	If not, does your program have unwritten policy to review data releases that are not covered under the standing data release policy? Describe briefly those procedures or policies:_____

STANDARD 3.6

☐ Yes ☐ No	Does your program routinely distribute nonidentifiable summary data to stakeholders?

STANDARD 3.7

☐ Yes ☐ No	Does your program assess data for quality before disseminated?

STANDARD 3.8

☐ Yes ☐ No	Does the program have a data-release policy that defines access to, and use of, individual-level information?
☐ Yes ☐ No	Does the data-release policy incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying information?

4.0 PHYSICAL SECURITY

STANDARD 4.1

☐ Yes ☐ No	Are workspaces and paper copies for persons working with confidential, individual-level information located within a secure, locked area? ☐ Are sensitive documents stored in cabinets? ☐ Are the cabinets locked? ☐ Are cabinets located in an area to which there is no access by unauthorized employees? ☐ Are cabinets located in an area to which there is no public access?

STANDARD 4.2

☐ Yes ☐ No	Do program staff members shred documents containing confidential information with a cross-cutting shredder before disposing of them?

STANDARD 4.3

☐ Yes ☐ No	Does your program have a written policy that outlines procedures for handling paper documents which could contain confidential information that are mailed to, or from, the program?

☐ Yes ☐ No	Do staff members in your program ensure that the amount and sensitivity of information contained in any piece of correspondence remains minimal?

STANDARD 4.4

☐ Yes ☐ No	Is access to all secured areas where confidential, individual-level HIV/VH/STI/TB/EPI/BT/Immunization information and data are stored limited to persons who are authorized within policies and procedures (this includes access by cleaning or maintenance staff)?

STANDARD 4.5

☐ Yes ☐ No	Do policies include procedures for securing documents containing PII when they cannot be returned to a secure work site by the close of business?
☐ Yes ☐ No	Do policies outline specific reasons, permissions and physical security procedures for using, transporting and protecting documents containing PII in a vehicle or personal residence?
☐ Yes ☐ No	If no such procedure exists, is approval obtained from the program manager?

STANDARD 4.6

☐ Yes ☐ No	When identifying information is taken from secured areas and included in on-line lists or supporting notes, in either electronic or hard-copy format: ☐ is it assured that the documents contain only the minimum amount of information necessary for completing a given task?, and ☐ is the information encrypted?, and ☐ is it coded to disguise information that could be easily associated with individuals?
☐ Yes ☐ No	Do staff members in your program ensure that terms easily associated with HIV/VH/STI/TB/EPI/BT/Immunization do not appear anywhere in the context of data transmissions, including sender and recipient addresses and labels?

5.0 ELECTRONIC DATA SECURITY

STANDARD 5.1

☐ Yes ☐ No	In your program, are HIV/VH/STI/TB/EPI/BT/Immunization analysis data sets stored securely using protective software (i.e., software that controls the storage, removal, and use of the data)?
☐ Yes ☐ No	Are personal identifiers removed from HIV/VH/STI/TB/EPI/BT/Immunization analysis data sets whenever possible?

STANDARD 5.2

☐ Yes ☐ No	In your program, do transfers of HIV/VH/STI/TB/EPI/BT/Immunization data and information and methods for data collection: ☐ have the approval of the ORP?, and ☐ incorporate the use of access controls?, and ☐ encrypt individual-level information and data before electronic transfer?

☐ Yes ☐ No	When possible, are databases and files with individual-level data encrypted when not in use?

STANDARD 5.3

☐ Yes ☐ No	Does your program have a policy that outlines procedures for handling electronic information and data (including, but not limited to, e-mail and fax transmissions) which may contain confidential information that are sent electronically to or from the program?
☐ Yes ☐ No	When individual-level HIV/VH/STI/TB/EPI/BT/Immunization information or data are electronically transmitted and transmission does not incorporate the use of an encryption package meeting the encryption standards of the National Institute of Standards and Technology and approved by the ORP, are the following conditions met? ☐ The transmission does not contain identifying information. ☐ Terms easily associated with HIV/VH/STI/TB/EPI/BT/Immunization do not appear anywhere in the context of the transmission, including the sender and recipient address and label.

STANDARD 5.4

☐ Yes ☐ No	For all laptop computers and other portable devices (e.g., personal digital assistants [PDAs], other handheld devices, and tablet personal computers [tablet PCs]), which receive or store HIV/VH/STI/TB/EPI/BT/Immunization information or data with personal identifiers, are all the following steps taken to ensure the security of the data? ☐ The devices have encryption software that meets federal standards. ☐ Program information with identifiers is encrypted and stored on an external storage device or on the laptop's removable hard drive. ☐ External storage devices or hard drives containing the information are separated from the laptop and held securely when not in use. ☐ The decryption key is kept some place other than on the device.
☐ Yes ☐ No	Do the methods employed for sanitizing a storage device ensure that the information cannot retrieved using "undelete" or other data retrieval software?
☐ Yes ☐ No	Does the program have policies or procedures to ensure that all removable or external storage devices containing HIV/VH/STI/TB/EPI/BT/Immunization information or data that contain personal identifiers: ☐ include only the minimum amount of information necessary to accomplish assigned tasks as determined by the program manager, and ☐ are encrypted or stored under lock and key when not in use, and ☐ are sanitized immediately after a given task (excludes devices used for backups)? Where are these policies or procedures stored?_____

☐ Yes ☐ No	Are hard drives that contain identifying information sanitized or destroyed before the computers are labeled as excess or surplus, reassigned to nonprogram staff members, or sent off site for repair?

STANDARD 5.5

☐ Yes ☐ No	Does your program have policies for handling incoming and outgoing facsimile transmissions to minimize risk of inadvertent disclosure of PII?

APPENDIX J – REPORTABLE DISEASES IN SOUTH DAKOTA

+Category I diseases: *Report immediately* on suspicion of disease
Category II diseases: Report within 3 days
★ Send isolate or specimen to South Dakota Public Health Laboratory

Effective Date: 1 January 2024

Acute flaccid myelitis
+Anthrax (*Bacillus anthracis*★)
Anaplasmosis (*Anaplasma phagocytophilum*)
Arboviral encephalitis, meningitis and **infection** (including, but not limited to, West Nile, Zika, St. Louis, Eastern equine, Western equine, Chikungunya, California, LaCrosse, Jamestown Canyon, Japanese, Powassan, Colorado tick fever)
Babesiosis (*Babesia* spp)
+Botulism (*Clostridium botulinum*)
+Brucellosis (*Brucella* spp★)
Campylobacteriosis (*Campylobacter* spp)
Carbon monoxide poisoning
Chancroid (*Haemophilus ducreyi*)
Chlamydia (*Chlamydia trachomatis*)
Cholera (*Vibrio cholerae*)
Coccidioidomycosis (*Coccidioides* spp)
+*Coronavirus* respiratory syndromes, MERS-CoV, SARS-CoV-1 and SARS-CoV-2
Cryptosporidiosis (*Cryptosporidium* spp)
Cyclosporiasis (*Cyclospora cayetanensis*)
Dengue viral infection (*Flavivirus*)
+Diphtheria (*Corynebacterium diphtheriae*★)
Drug resistant organisms:
- **Carbapenemase-Producing Organisms** (CPO★)
- ***Candida auris***★
- **Vancomycin–intermediate & resistant *Staphylococcus aureus*** (VISA, VRSA★)

+*E. coli*, shiga toxin-producing (*Escherichia coli*★)
Ehrlichiosis (*Ehrlichia* spp)
Giardiasis (*Giardia lamblia / intestinalis*)
Gonorrhea (*Neisseria gonorrhoeae*)
***Haemophilus influenzae*★**, invasive disease
Hantavirus pulmonary syndrome or **infection**
Hemolytic uremic syndrome
Hepatitis, viral, acute **A, B** and **C**; chronic **B** and **C**; and perinatal **B** and **C**

Human immunodeficiency virus (HIV) **infection**, including:
- Stage III, Acquired immunodeficiency syndrome, (AIDS)
- CD4 counts in HIV infected persons
- HIV viral loads,
- pregnancy in HIV infected females,
- HIV gene sequencing
- HIV antiviral resistance,
- Confirmatory results, positive or negative, following a reactive HIV screening test

+Influenza, novel strains★
Influenza: including:
- hospitalizations,
- deaths,
- lab confirmed cases (culture, DFA, PCR),
- weekly aggregate totals of rapid antigen positive (A and B) and total tested

Lead, all blood levels
Legionellosis (*Legionella* spp)
Leprosy / Hansen's disease (*Mycobacterium leprae*)
Leptospirosis (*Leptospira*)
Listeriosis (*Listeria monocytogenes*★)
Lyme disease (*Borrelia burgdorferi*)
Malaria (*Plasmodium* spp)
+Measles / Rubeola (*Paramyxovirus*)
Melioidosis (*Burkholderia pseudomallei*)
+Meningococcal disease, invasive (*Neisseria meningitidis*★)
Mumps (*Paramyxovirus*)
+Orthopoxviruses (Variola★ or mpox virus)
Paratyphoid fever
Pertussis (*Bordetella pertussis*)
Pesticide-related illness and **injury,** acute
+Plague (*Yersinia pestis*★)
+Poliomyelitis, paralytic and nonparalytic (*Poliovirus*)
Psittacosis (*Chlamydophila psittaci*)
Q fever (*Coxiella burnetii*)
+Rabies, human and animal (*Rhabdovirus*)
+Rubella and congenital rubella syndrome (*Togavirus*)
Salmonellosis (*Salmonella* spp★)
Shigellosis (*Shigella* spp★)
Silicosis

Spotted fever rickettsiosis (*Rickettsia*)
***Streptococcus pneumoniae*, invasive**
Syphilis (*Treponema pallidum*) including primary, secondary, latent, early latent, late latent, neurosyphilis, late non-neurological, stillbirth, and congenital
Tetanus (*Clostridium tetani*)
Toxic shock syndrome (Streptococcal and non-Streptococcal)
Transmissible spongiform encephalopathies, such as Creutzfeldt-Jakob disease
Trichinosis (*Trichinella spp.*)
+Tuberculosis, active disease or **latent infection** (*Mycobacterium tuberculosis*★ *or Mycobacterium bovis*★)
(**Latent TB Infection** only in certain high risk persons: foreign-born <5 yrs in US, close contacts, diabetes, renal dialysis, children <5 yrs, and certain medical conditions)
+Tularemia (*Francisella tularensis*★)
Typhoid (*Salmonella typhi*★)
Vaccine Adverse Events
Varicella / Chickenpox (*Herpesvirus*)
+Viral Hemorrhagic Fevers (Crimean-Congo Hemorrhagic Fever virus, Ebola virus, Lassa virus, Lujo virus, Marburg virus, Chapre virus, Guanarito virus, Junin virus, Machupo virus, Sabia virus)
Vibriosis (*Vibrionaceae*★)
+Yellow fever (*Flavivirus*)

- - - - - - - - - - - - - - -

+Outbreaks of:
+Acute upper respiratory illness
+Diarrheal disease
+Foodborne disease
+Healthcare-associated infections
+Illnesses in child care setting
+Rash illness
+Waterborne disease

+Syndromes suggestive of **bioterrorism** and other **public health threats**
+Unexplained illnesses or **deaths** in human or animal

APPENDIX K – BREACH REPORT FORM

(Breach Reporting Form Instructions can be found in Appendix L)

A breach is the use of or disclosure of protected health information in violation of program policies and job responsibilities

Section 1: Initial Report (To be completed by the person receiving the initial notice of the suspected breach)

Type of Breach:

☐ Unauthorized Release of Information

☐ Unauthorized Access of Information

Date and Time of Breach

Date: Click or tap to enter a date. **Time:**

Location Where Breach Occurred:

Organization Name:

Address:

City:

State:

Type of Data which was compromised:

☐ Personally identified individual record-level data

☐ Pseudo-anonymized Data

☐ Aggregate Data

Means of unauthorized Access or Release of Information:

☐Building security

☐Field investigation

☐Workstation

☐Handling confidential mail

☐Telephone

☐Electronic data storage

☐Electronic data transmission

☐Faxing (facsimile) records

☐Email

☐Routine sharing of data

☐Laptops

☐Removable storage devices

☐GPS systems

☐Personal storage devices

☐Wi-Fi/blue tooth

☐Other:

Person Submitting This Report:	
Name:	**Agency/Affiliation:**
Work Phone:	**E-Mail Address:**
Date Submitted:	**Time Submitted:**
Signature: **(electronic accepted)**	
Person Who Released or Accessed the Unauthorized Information:	
Name:	**Agency/Affiliation:**
Work Phone:	**E-Mail Address:**
Title:	

Section 1: Initial Report
Describe the Suspected Breach that Occurred:

Describe contributing causes to the incident:

Section 2: Closing Report (To be completed by Security Team)

Did a breach in protocol occur? ☐ Yes ☐ No

Did a breach in confidentiality occur? ☐ Yes ☐ No

Was the breach due to negligence or purposeful in nature? ☐ Negligence ☐ Purposeful ☐ Unknown

If unknown, please explain why unknown?

Has confidential information been compromised? ☐ Yes ☐ No ☐ Unknown

If yes, what information has been compromised?

If no or unknown, please elaborate on your response?

Conclusions:

Immediate Recommendations:
(corrective actions)

Long-Term Recommendations:
(corrective actions)

Is follow-up action needed: ☐ Yes ☐ No

Section 3: Follow-up Report (To be completed by State Epidemiologist.)
Were any disciplinary actions or corrective actions taken to prevent the breach from occurring again? ☐ Yes ☐ No **If yes, then please describe the disciplinary and/or corrective actions that have been taken monthly to prevent the breach from occurring again.**

This incident has been investigated, the proper officials have been notified, and the corrective actions have been implemented in the event a breach has been confirmed.

Section 4: Final Signatures	
Signature: (when appropriate) (electronic accepted)	**Date:**
Typed Name:	

I have reviewed and approved the resolution of this investigation and actions taken.

ORP Signature(s): (electronic accepted)	**Date:**
Typed Name:	

APPENDIX L – REPORTING A SUSPECTED BREACH

1.	The staff member, contractor or IT person reporting the initial notice of the suspected breach will document the incident using the Breach Report Form (Appendix K: "Section 1, Initial Report").
2.	The initial breach report must be completed and submitted via email to the employee's direct supervisor (with advance notice of the occurrence), the Director of ID Informatics, and the ORP within 24 hours of the incident. If the direct supervisor is unavailable, notify the Deputy State Epidemiologist. If the Deputy State Epidemiologist is also unavailable, notify the Deputy Administrator of ODPS Programs via email.
3.	The staff person, contractor, or IT person who reported the suspected breach must receive an e-mail confirmation from one of the above parties indicating receipt and review of the initial Breach Report Form. If no confirmation is received the staff member, contractor, or IT person who reported the suspected breach; the initial Breach Report Form must then be sent directly to the ORP.
4.	The Director of ID Informatics and ORP will review the initial Breach Report and make a recommendation to the direct supervisor for closing out the report when sufficient and reasonable information confirms that a breach has not occurred.
5.	The Director of ID Informatics, ORP and any staff, contractor, or IT person as appropriate with the initial breach report via email within 24 hours after receiving the completed initial Breach Report Form from the staff member, contractor, or IT person.

Investigating a Suspected Breach

1.	After the direct supervisor has received the breach report, the direct supervisor will inform the Director of ID Informatics and ORP of the suspected breach.
2.	The Security Team (Director of ID Informatics, ORP, and direct supervisor) will be responsible for further investigating the incident. (The Security Team may request further information regarding the incident to be submitted.)
3.	The Security Team will review the initial breach report and complete "Section 2: Security Team Closing Report". The investigation should be finished no later than 7 days following the initial incident date.
4.	The final completed report (Sections 1 and 2) will be sent to the ORP via e-mail.
5.	All media calls related to a suspected breach must be referred to the Public Information Officer at 605-773-3361.
6.	Any breach of confidentiality will be investigated immediately to assess causes and implement corrective actions. If a breach of confidentiality is related to a federally sponsored program, the ORP may report it to the appropriate federal program contact. Please see section 1.5.

Action Steps Specific to the Type of Breach

1.	Suspected Breach (Non-breach in protocol): a. A suspected breach is reported, and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is neither a breach of protocol nor a breach of confidentiality. c. The Security Team communicates the findings to the appropriate contractor, IT or staff member. d. The Security Team will be responsible for closing out the report.

2.	Breach in Protocol: a. A suspected breach is reported, and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is a breach in protocol but not a breach in confidentiality. (In this case the Security Team has determined that no confidential information has been divulged in any manner, but a breach in protocol poses a risk to a breach in confidentiality and recommendations will need to be made accordingly.) c. When only a breach in protocol has occurred, the Security Team will need to determine if the breach was negligent or purposeful. d. The Security Team will recommend the necessary actions to be taken based on the type of breach (negligent or purposeful). e. Subsequently, it is the responsibility of the DPC to monitor the employee or contractor and assure that further breaches in protocol do not occur that may ultimately result in a breach of confidentiality. f. The DPC will also assure that the employee causing this breach in protocol receives emergency training on security and confidentiality. g. Additionally, disciplinary action may need to be taken especially when repeated breaches in protocol have occurred. If the employee or contractor continues to pose a threat to security of confidentiality, the employee's or contractor's access to surveillance information will be limited or rescinded until further personnel actions have been determined.
3.	Breach in protocol and confidentiality: a. A suspected breach is reported, and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is a breach in protocol and a breach in confidentiality. (In this case the Security Team has determined that confidential information has been divulged, and an immediate response is necessary.) c. When the suspected breach is found to be both a breach of protocol and breach of confidentiality, the Security Team will make appropriate recommendations regarding actions that will need to be taken based on whether the breach is determined to be purposeful or due to negligence. d. Regardless of the type of breach (purposeful or negligent), the following recommendations may be required based on the severity of the breach of confidentiality: o The contractor or employee's access to physical and electronic resources must be limited or rescinded until an investigation of the incident is complete. Options for handling the situation include immediately reassigning the employee to a temporary duty station; obtaining permission from the Supervisor (to whom the employee is assigned) or ORP to send the employee home pending investigation of the breach; or calling law enforcement in extreme situations. o At the discretion of the ORP the following entities may be notified: legal counsel, the Secretary of Health, appropriate federal authorities, such as HRSA, CDC and ISSO, if appropriate. o Implement new or additional processes to address any deficiencies in the program security and confidentiality policies and procedures.

Follow-Up to a Breach and Maintenance of Files

1.	If a breach has occurred, the direct supervisor will submit a follow-up report via e-mail to both Director of ID Informatics and ORP monthly. The follow-up report will detail the corrective steps (Section 3 of Breach Report Form) that have been taken to resolve the problem to prevent the breach from occurring again.
2.	Monthly, the Director of ID Informatics and the ORP will confirm receipt of the follow-up Breach Report Form and indicate if the response is appropriate. Monthly follow-up reports will be submitted until corrective actions are concluded or deemed sufficient by the ORP.
3.	The ORP or designee will retain a file of all completed breach response forms in a locking file cabinet. (Breach Report Forms will be maintained separate from the employee's personnel file.)
4.	The ORP's designee will enter all information into the Breach Report Database. The Breach Report Database will be password protected.
5.	The direct supervisor will be responsible for periodically running reports based on the Breach Report Database and determine if any patterns in breaches exist that need to be further addressed.

Breach Reporting Form Instructions

Section 1: This section is to be completed by the person who initially identified the breach (e.g. received an email with confidential information, found forms in trash that should have been shredded, lost their documents, etc.)

Type of Breach:

Unauthorized Release: Confidential information was provided to someone that should not have. This is the most common and usually involves emails, faxes, misplaced documents, etc.

Unauthorized Access: Someone without proper authorization was given access to confidential information. Examples include an individual allowed into a secure area without authorization, given access to data files without approval, hacking, stolen or using someone else's password, etc.

Date: m/d/yyyy **Time:** h:mm am/pm (approximate)

Type of Data compromised:

Personally identified individual record level: information which, when combined with other information, could potentially identify an individual or individuals. This includes but is not limited to such information as medical record/case numbers and demographic or locality information that describe a small subset of individuals (e.g., block data, zip codes, race/ethnicity data).

Pseudo-anonymized data: individual record-level data which has been stripped of personal identifiers (e.g., name, address, social security number) but may contain potentially identifying information (e.g., age, sex, race/ethnicity, locality information) that when combined with other information may identify an individual. If the combining of information could identify an individual, these data are considered confidential.

Aggregate Data: data which are based on combining individual level information; Aggregate data may contain potentially identifying information, particularly if the aggregated data are very detailed or for a small subset of individuals.

Means of Unauthorized Access or Release of Information: check all that apply.

Person Submitting This Report: This is typically the person who is reporting the breach but may also be their manager or surveillance program manager. This may be the same person who released the information.

Person Who Released or Accessed the Unauthorized Information: Person who caused the breach. This may be the same as the person reporting.

Describe the suspected breach that occurred: Please be detailed here.

Describe contributing causes to the incident: Was the person new? Had they received the training? In a hurry? What types of things may have contributed to the breach happening?
After completing Section 1, please send to the direct supervisor and to Director of ID Informatics and the ORP. Please see **Appendix E**.

Section 2: Closing Report
This section will be completed with the direct supervisor. They may consult with the person's involved in the incident, the Director of ID Informatics and the ORP. It may take more pages than this report

allows including all the information and additional pages will be submitted as part of this document in closing.

Section 3: Follow Up Report
This section to be completed by the Director of ID Informatics or the ORP, depending on the nature of the breach other authorities including legal authorities, federal sponsors, agency management and legal authorities.

Section 4: Final Signatures
The ORP will sign off as appropriate.

APPENDIX M – STATE OF SOUTH DAKOTA REMOTE WORK OFFICE SAFETY CHECKLIST

State of South Dakota Remote Work Office Safety Checklist

The remote work employee **must read and complete** this checklist regarding the remote work office area, discuss any concerns, and always report accidents or injuries immediately to his/her supervisor. If the answer to any question below is "no", a remote work arrangement may not be approved until the condition(s) is remedied.

Safety Conditions	Yes	No
Is the workspace away from noise and distractions, and is the workspace devoted to the employee's needs?	☐	☐
Does the space seem adequately ventilated?	☐	☐
Is the space reasonably quiet?	☐	☐
Are all stairs with four or more steps equipped with handrails?	☐	☐
Are all circuit breakers and/or fuses in the electrical panel properly labeled?	☐	☐
Do circuit breakers clearly indicate if they are in open or closed position?	☐	☐
Is all electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, loose wires, flexible wires running through walls, exposed wires fixed to the ceiling, away from heat sources)?	☐	☐
Are electrical outlets three-pronged (grounded)?	☐	☐
Are hallways, doorways and corners free of obstructions to permit visibility and movement?	☐	☐
Are file cabinets and storage closets arranged so drawers and doors do not open into walkways, and file drawers are not top-heavy?	☐	☐
Do chairs appear sturdy?	☐	☐
Is the space free of clutter or excessive furniture?	☐	☐
Are the phone lines, electrical cords and extension wires secured under a desk or alongside a baseboard?	☐	☐
Is the office space neat and clean?	☐	☐
Are floor surfaces clean, dry, level, and free of worn or frayed seams?	☐	☐
Are carpets well secured to the floor and free of frayed or worn seams?	☐	☐
Is there a fire extinguisher in the area, easily accessible from the office space (required)?	☐	☐
Is there a working (test) smoke detector within hearing distance of the workspace (required)?	☐	☐
Are all radiators and portable heaters located away from flammable items?	☐	☐
Is there an evacuation plan in place in the event of a fire or other emergency?	☐	☐
Is lighting adequate?	☐	☐
Is all computer equipment connected to a surge protector?	☐	☐
Is the workstation ergonomically adequate (arm rests, leg room, back support, screen level)?	☐	☐
Is there high quality, reliable cell phone and internet connectivity in the workspace?	☐	☐
Other:	☐	☐
Comments:		

Agreement

I_____, understand it is my responsibility to maintain the safety and appropriate arrangement of my remote work office area. I certify that my responses to the checklist are true and complete to the best of my knowledge. I understand that any erroneous, misleading, or fraudulent information will cause my preclusion from remote working.

Employee: _____ Date: _____

Supervisor: _____ Date: _____

APPENDIX N – AUTHORIZATION FOR OFFSITE ACCESS TO SDEDSS

The Overall Responsible Party (ORP) must approve all offsite access to SDEDSS. Offsite access is defined as any computer access point that is not directly serviced through a Bureau of Information and Telecommunication local access network terminal in a State-owned or State-designated facility. Offsite access can only be granted for temporary service for ensuring continuity of critical Department of Health functions. Approval is required each time offsite access is requested and is only effective for the dates specified.

Date of Request: _____

Employee Name: _____

Offsite Location Name: _____

Offsite Location Description: _____

_____

Offsite Physical Address: _____

Offsite Access From Date: _____

Offsite Access To Date: _____

By signing, the employee understands and assures all confidentiality and security requirements will be met and maintained through the duration of offsite service.

Employee Signature_____ Date_____

Supervisor Signature: _____ Date_____

ORP Signature: _____ Date_____

APPENDIX O – SDDOH SECURITY AND CONFIDENTIALITY PROGRAM REQUIREMENT CHECKLIST

Person completing form (please print): _____

Title: _____ Date: _____

Sign your name: _____

Program Area/Job Title: _____

Requirements (Initial items as completed)

___ Requirement 1: Policies must be in writing. (1.0)

___ Requirement 2: Policies must be readily accessible by any staff having access to confidential surveillance information or data at the central level and, if applicable, at noncentral sites. (1.1)

___ Requirement 3: A policy must name the individual who is the Overall Responsible Party (ORP) for the security system. (1.2)

___ Requirement 4: In compliance with CDC's cooperative agreement requirement, the ORP must certify annually that all program requirements are met. (1.2)

___ Requirement 5: A policy must clearly outline the roles of all individuals authorized to access specific types of information and establish the standard procedures or methods to be followed for staff outside the surveillance unit when access is deemed necessary. (1.3)

___ Requirement 6: A policy must describe methods for the review of security practices for HIV/AIDS surveillance data. Included in the policy should be a requirement for an ongoing review of evolving technology to ensure that data remain secure. (1.4)

___ Requirement 7: All authorized personnel with access to surveillance data are responsible for reporting any suspected security breaches. This requirement must also be included in the training provided to non-surveillance staff. (1.5)

___ Requirement 8: Any breach of confidentiality must be promptly investigated to determine the cause and implement appropriate corrective actions. (1.5)

___ Requirement 9: Any breach that leads to the disclosure of private information about one or more individuals (a breach of confidentiality) must be reported immediately to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. The CDC may provide support to the surveillance unit handling the incident. In coordination with appropriate legal counsel, surveillance staff should assess whether the breach should be reported to law enforcement agencies. (1.5)

___ Requirement 10: All individuals with access to surveillance data are required to complete annual security training. The date of their initial training must be recorded in their personnel file. IT staff and contractors who need access to data must complete the same training as surveillance personnel and

sign the same confidentiality agreements. This requirement applies to anyone with access to servers, workstations, backup devices, or similar systems. (1.6)

___ Requirement 11: All authorized personnel are required to sign a confidentiality statement annually. Newly hired or newly authorized staff must sign this statement before being granted access to surveillance data. They must present the signed statement to the individual responsible for issuing passwords and keys prior to receiving access. The statement must affirm that the employee understands and agrees not to disclose surveillance data or information to anyone not authorized by the ORP. The original signed statement must be kept in the employee's personnel file. (1.7)

___ Requirement 12: Every member of the surveillance team and all individuals authorized to access case-specific information, as outlined in this document, must be well-informed about the organization's information security policies and procedures. Additionally, all authorized staff are responsible for questioning anyone who attempts to access surveillance data without proper authorization. (1.8)

__ Requirement 13: All authorized staff members are personally responsible for securing their workstations, laptops, or any other devices used to access confidential surveillance information or data. This includes safeguarding keys, passwords, and access codes that provide entry to sensitive information. Staff must also take precautions to prevent introducing computer viruses to surveillance software and avoid damaging hardware by exposing it to extreme temperatures. (1.8)

___ Requirement 14: Simultaneous access of SDEDSS and public internet websites should not occur. Care should be taken when using email applications (e.g. Outlook) and SDEDSS simultaneously to ensure sensitive or confidential information is not inadvertently transmitted. When using Outlook to communicate sensitive or confidential information, users must use secure email settings within Outlook. (1.8)

___ Requirement 15: Access to surveillance information containing names for research purposes (beyond routine surveillance) must be granted only when there is a demonstrated need for the names, Institutional Review Board (IRB) approval has been obtained, and a confidentiality statement outlining access rules and final disposition of the information has been signed. Access to surveillance data without names for research purposes outside of routine surveillance may also require IRB approval, depending on the number and type of variables requested, in accordance with local data release policies. (2.4)

___ Requirement 16: Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP. (3.1)

___ Requirement 17: Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document. (3.3)

___ Requirement 18: Access to surveillance information or data for nonpublic health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law. (3.4)

___ Requirement 19: Access to and uses of surveillance information or data must be defined in a data release policy. (3.8)

___ Requirement 20: A policy must incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying. (3.8)

___ Requirement 21: All physical locations containing electronic, or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area. Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room (4.1)

___ Requirement 22: Accessing SDEDSS during business travel, users must use the secure Citrix Application, be in a private secure room while working in SDEDSS. Users must log off SDEDSS and Citrix or lock the computer, when not present in the room. (4.1)

___ Requirement 23: Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the ORP. (4.1)

___ Requirement 24: Prior approval must be obtained from the ORP when planned business travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day. (4.1)

___ Requirement 25: Each member of the surveillance team must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature. (4.2)

___ Requirement 26: A policy must establish procedures for managing both incoming and outgoing mail within the surveillance unit. The volume and sensitivity of information included in each piece of mail should be minimized. (4.3)

___ Requirement 27: Rooms containing surveillance data must not be easily accessible by window. (4.3)

___ Requirement 28: Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP. (4.4)

___ Requirement 29: When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV(900), AIDS(950), Syphilis(700), GC (300) and Chlamydia (200). (4.5)

___ Requirement 30: Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area. (4.5)

___ Requirement 31: An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data). (5.1)

___ Requirement 32: Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use. (5.2)

___ Requirement 33: When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label. (5.3)

___ Requirement 34: Laptops, tablets and other portable devices that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards. (5.4)

___ Requirement 35: Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing before reuse. If the machine is coming through surplus, it will be wiped/sanitized. If the machine is not coming through surplus and needs to be wiped, make request through the Help Desk asking that a 3-pass wipe of the hard drive be performed. (5.5)

APPENDIX P – SDDOH HIPAA POLICY STATEMENT

Refer to the DOH Procedure and Form Manual here.

The Department of Health (DOH) shall require its workforce members (including management at all levels) to complete HIPAA training. All new employees will complete the New Hire HIPAA training within thirty (30) days of their employment, and sign and return the DOH "Confidentiality Agreement" and the BHR HIPAA Training Verification forms to their supervisor. All DOH employees must also complete annual HIPAA training.

Procedure

A. DOH HIPAA training shall ensure that workforce members are familiar with DOH's HIPAA privacy policies and procedures for protecting client and program participant privacy and securing PHI. Training shall enable DOH workforce members to understand the impact of PHI privacy and security on their day-to-day functions.

B. DOH requires its workforce members, whose functions are affected by a material change in the DOH HIPAA privacy policies or procedures, to be trained within a reasonable period of time after the material change becomes effective.

C. Training shall include information about responsibilities and accountability, including the sanctions exercised for non-compliance ranging from disciplinary actions to termination of employment.

D. The new hire employee will sign and submit the BHR training verification form and DOH Confidentiality Agreement to their supervisor within thirty (30) days of their employment.

E. Employees can find a copy of the DOH Confidentiality Agreement form on the SD DOH Intranet located here. The verification form will be obtained at the conclusion of the BHR HIPAA training.

F. A signed copy of the employee's Confidentiality Agreement and BHR Verification of HIPAA Training forms shall be kept in each employee's file.

APPENDIX Q – SDDOH HIPAA CONFIDENTIALITY AGREEMENT

I, _____, have been trained and informed of the Administrative Policies and Procedures of the Department of Health (DOH) as related to the Health Insurance Portability and Accountability Act (HIPAA). The DOH places a high priority on maintaining the confidentiality of its program participant's information. I understand that I must ensure the privacy of program participants protected health information (PHI) held by the DOH. I understand that non-compliance with the DOH Administrative Policies and Procedures is cause for disciplinary action up to and including dismissal from the DOH, as well as possible legal actions for any criminal or civil violations of applicable HIPAA regulations. I agree to promptly report all violations, or suspected violations, of any of the DOH Administrative Policies and Procedures to my direct supervisor and the Department of Health HIPAA Compliance Officer.

DOH Employee/Contractor/Student/Volunteer Signature and Date

Print Name

DOH Supervisor Signature and Date