SOUTH DAKOTA DEPARTMENT OF HEALTH

Office of Disease Prevention and Health Promotion AND Epidemiology, Surveillance, and Informatics Center Data Security and Confidentiality Manual

Contents

1.0 PROGRAM POLICIES AND RESPONSIBILITIES

This data security and confidentiality manual has been established to ensure data security, confidentiality, and use across surveillance and program areas for Human Immunodeficiency Virus (HIV), Ryan White, Sexually Transmitted Diseases (STD), Tuberculosis (TB) and other communicable diseases (EPI) prevention. South Dakota state law 34-22-12 requires mandatory communicable disease reporting to the Department of Health (DOH) by physicians, hospitals, laboratories, and institutions. The public has a right to privacy under U.S. constitutional amendments, the Public Health Service Act, South Dakota state law 34-22-12, and Department of Health, Administrative Policies and Procedures, Statement No. 25, issued: November 1, 2006, revised April 22, 2016 Title: HIPAA – Business Associates, Statement No. 26 issued: April 22, 2016, revised September 18, 2018. Please see Appendix C and D.

National program requirements to protect HIV, Viral Hepatitis, Sexually Transmitted Disease and Tuberculosis 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, National Center for HIV/AIDS, Viral Hepatitis, STD and TB Prevention. 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. 2012.

1.1 POLICIES AND PROCEDURES

South Dakota Department of Health, the Office of Disease Prevention and Health Promotion (ODPHP) and Epidemiology, Surveillance, and Informatics Center (ESIC) used these requirements to develop this data security and confidentiality policy manual, which is implemented throughout the programs and diseases and is reviewed annually.

The 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: http://doh.sd.gov/diseases/infectious/HIV-AIDS/data-confidentiality.aspx.

Only DOH personnel and program contractors who have a need-to-know will have access to disease-specific surveillance data with identifiers. The two surveillance unit Overall Responsible Parties (ORPs) are the Division Director of Family and Community Health and State Epidemiologist. The surveillance unit under the Division of Family and Community Health consists of the Administrator of the ODPS, Program Managers (responsible for the HIV/AIDS Reporting System [eHARS]), Deputy Administrator, Regional Supervisors, ODPHP Secretaries, SD-DOH Disease Intervention Specialists (DIS), HIV Case Management, and Community Health Services Staff. The surveillance unit under the Epidemiology, Surveillance, and Informatics Center consists of the Deputy State Epidemiologist, Director of Infectious Disease Informatics, epidemiologists, and informaticians (responsible for the South Dakota Electronic Disease Surveillance System [SDEDSS]. Common to both surveillance units are the South Dakota Bureau of Information Database Administrators. Please see Table 1 (Appendix E).

The Program Managers are located in the central and field offices and are responsible for writing grant applications, case management within SDEDSS, assigning disease case investigations to the DIS, dissemination of surveillance data, and transferring data to CDC. The DIS are located across the state in field offices and are responsible for all case investigations, active case finding, and case follow-up. Contractors are responsible for case management services, case investigation, Ryan White services, linkage to care services, SDEDSS support services or data evaluation and are in multiple cities across the state including Sioux Falls, Pierre, Mitchell, Aberdeen, Watertown, Winner, and Rapid City. Facilities are State approved facilities.

In addition to the above roles, the HIV/AIDS surveillance coordinator and the linkage to care coordinator are responsible for maintaining the HIV/Acquired Immunodeficiency Syndrome (AIDS) Reporting System (eHARS) database.

1.2 OVERALL RESPONSIBLE PARTY (ORP)

As part of the program requirements, the Director of the Division of Family and Community Health, Beth Dokken, is designated as the ORP for ODPHP. Josh Clayton is designated as the ORP for Epidemiology, Surveillance, and Informatics (ESIC). The ORPs have the responsibility for the security of the HIV surveillance system (eHARS) and the South Dakota Electronic Disease Surveillance System (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 used for all communicable disease surveillance and case management. SDEDSS security standards meet the established HIPAA (Health Insurance Portability and Accountability Act) standards. Each SDEDSS user is assigned a unique username and password. Associated with each user profile are one or more roles, which determine the permissions and access restrictions that the user has for different parts of the system functionality. Users are also affiliated with groups which control which events a particular user can access.

Access to surveillance information with identifiers by those who maintain other disease registries (ex. TB, STD, EPI) will be limited to Program Managers in the Office of Disease Prevention and Health Promotion or epidemiologists in ESIC for whom the level of security is equivalent to the standards described in this document. Only information necessary to provide public health services or medical care will be shared.

Access to patient records will be limited to surveillance activities only by those authorized by the corresponding program manager, epidemiologist, or ORP.

Only authorized individuals can: Access the information systems (network logon, establish connection); Activate specific system commands (execute specific programs and procedures); create, view, or modify specific objects, programs, information system parameters. Please see Table 1 (Attachment F).

The Director of Infectious Disease Informatics and/or the HIV Surveillance Coordinator 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 statewide ORP.

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

3. Manage a list of specific authorized staff (Attachment F) 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 viewers.

1.4 ANNUAL TECHNOLOGY REVIEW AND BACKUP/RECOVERY PLAN

An annual review of evolving technology to ensure that the data security policies and procedures remain secure will be performed by the HIV Surveillance Coordinator, Director of Infectious Disease Informatics, and the SD-BIT point of contact. Please see Revision Table on page 20.

The Director of Infectious Disease Informatics and HIV Surveillance Coordinator will evaluate and ensure that the data security policies and procedures meet CDC program requirements by assessing the "Assessment Checklist" shown as Appendix I on an annual basis.

When any security changes to information systems technology are proposed, the SD-BIT point of contact, HIV Surveillance Coordinator, and Director of Infectious Disease Informatics are responsible for collaborating with the Program Managers to prepare technical solutions. This collaboration will help ensure that in no way the security and confidentiality of communicable disease surveillance data are electronically 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 in order 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.

Backup Information

Full backups are taken each evening for all production databases on servers for ADABAS, Oracle and MS SQL SERVER.

Backups for Oracle and MS SQL Server are maintained on a 62-day cycle.

Backups for ADABAS are maintained on a 5-day cycle.

Backups are maintained for a 13-month cycle.

Database log files, archive files, and protection logs are backed up throughout the day as needed and then copied to tape and taken off- line for off-site storage. The files are retained for 62-days.

Each night drives are backed up on campus and then sent encrypted to a secure location.

1.5 SECURITY BREACHES

All staff authorized to access surveillance data are responsible for reporting suspected security breaches. Training of non-surveillance staff will also include this directive. A breach of security must be immediately reported to the respective ORP. In the event of a suspected electronic data breach, BIT should be also notified immediately. Documentation of the breach will be maintained by the ORP describing the investigation findings and corrective actions taken. A breach of confidentiality will be immediately investigated to assess causes and implement remedies.

A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the respective ORP. The breach will then be reported by the respective ORP to the appropriate Center for Disease Control and Prevention (CDC) staff, such as the CDC Program Manager, DHAP, NCHSTP, and HRSA Program Manager. In consultation with appropriate legal counsel, the ORP will determine whether a breach warrants report to law enforcement agencies. Please see Breach Report Form (Appendix K).

To minimize the risk of security breaches regarding surveillance data and PII, staff must use at least two methods to confirm client identity (i.e. name and birthdate).

1.6 ANNUAL SECURITY TRAINING

Every individual with access to communicable surveillance data must attend annual data security training. This requirement applies to any IT staff, staff with access to servers, workstations, backup device, etc. All individuals who require access to data must undergo the same training and sign the same agreements. There are no job-specific trainings. The original date of training must be documented in the employee's personnel file.

Trainings will cover the data security and confidentiality standards in this document, including the review of the physical and electronic data security, confidentiality procedures and release and sharing procedures. The training materials include this document, which will be updated as needed.

Each individual must annually electronically sign a confidentiality statement. 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 given to the employee. All subsequent statements will be placed in a working file. Please see Appendix B.

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 the new-hire 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 given to the employee. Please see Appendix B.

After the initial training, the individual will then follow the Annual Security Training requirements above (1.6).

1.8 INDIVIDUAL SECURITY RESPONSIBILITIES

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 South Dakota Department of Health's data security and confidentiality policies and procedures and will be required to annually perform the Data Security and Confidentiality Program Requirement Checklist. Please see Appendix O.

Each individual has the following general responsibilities pertaining to the data security and confidentiality of communicable disease surveillance information.

1. Challenging unauthorized users of communicable disease surveillance data. Authorized users and authorized use of communicable disease surveillance information are defined in Appendix F of this manual.

2. Immediately reporting all suspected breaches of confidentiality to the ORPs, Administrator of the Office of Disease Prevention Services (ODPHP), Deputy Administrator of ODPHP, Deputy State Epidemiologist, and the respective Program Manager or epidemiologist. The ORP or the designee of the ORP will report breaches to the appropriate CDC Team Leader, Program Consultant, and Epidemiologist.

3. Exercising good judgment in the daily management of communicable disease surveillance information. From time to time, data security and confidentiality issues related to communicable disease surveillance data may arise that are not specially addressed in this manual. When these issues arise, the surveillance staff is responsible for notifying the ODPHP Administrator, Director of Infectious Disease Informatics, and the appropriate Program Manager or epidemiologist who can provide the necessary guidance related to these issues.

4. All staff authorized to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold.

5. All surveillance staff should avoid situations that might allow an unauthorized person to overhear or see confidential surveillance information. For example, staff should never discuss confidential surveillance information in the presence of persons who are not authorized to access the data. Paperwork and computer monitors should not be observed by unauthorized personnel.

6. Ideally, only staff with similar roles and authorizations would be permitted in a secure area.

7. Incoming telephone calls will be answered with generic identifiers (e.g., “Department of Health”, “This is Christine”), without any direct reference to specific diseases.

8. Outgoing calls requesting confidential information to perform routine disease surveillance activities will be conducted in a manner that does not allow phone conversations to be overheard. Messages with identifying patient identifiers are not left on voice mail systems unless there is prior confirmation of a secure line. Staff should discuss confidential information only in secure areas, release information to only those individuals with a need-to-know and always use utmost discretion.

9. Simultaneous 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 to users outside of DOH firewall, users must use secure email (e.g. Voltage).

2.0 DATA COLLECTION AND USE

2.1 DATA USE PURPOSE

The collection of Public Health data is to prevent disease and promote health among South Dakota citizens. This data will be used to assess the health needs and health status of South Dakota and its communities through Public Health surveillance and epidemiologic research; develop public health policy; develop public health needs and emergencies; and evaluate public health programs.

2.2 MINIMUM DATA

Minimum data requirements are stated in our ODPHP and ESIC policy and procedure manual. The minimum data information is collected to complete and achieve our public health goals. The ODPHP policy and procedure manual can be found at: M:\DOH\Disease Prevention\ODP\EPI Manual\Policies.

2.3 PERSONAL IDENTIFYING INFORMATION

Personal Identifiable Information (PII) is collected and used only when necessary for public health prevention purposes. De-identifiable information is used for analysis and reporting purposes.

2.4 PUBLIC HEALTH RESEARCH

Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names and Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without name for research purpose beyond routine surveillance may still require IRB approval depending on the numbers and type of variables requested. All requests should be directed to the respective ORP for direction.

3.0 DATA SHARING AND RELEASE

3.1 ORP APPROVAL

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 respective ORP.

3.2 RISK & BENEFIT ASSESSMENT

When proposed sharing of identifiable data is not covered by existing policies, the respective ORP will assess the risks and benefits before deciding to share the data.

3.3 PROGRAM-SPECIFIC DATA SECURITY

Disease programs outside the primary program responsible for collecting and storing the data have limited access to the primary program’s data. The respective ORP has evaluated and weighed the benefits and risks of allowing this limited access; and the necessary levels of security within SDEDSS have been established.

Individuals that carry the on-call phone will have approval through the respective ORP to access SDEDSS offsite. Access is given for one year at a time and staff will follow the security protocols identified in this document.

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

Access to any surveillance information containing identifiers is not allowed outside the surveillance unit except for the provisions covered under SDCL 34-22-12.1 and with the respective ORP approval. Access to surveillance data or information without names may still require the respective ORP approval depending on the numbers and types of variables requested and in accordance with data release policies.

3.6 DISSEMINATION OF DATA

The State Epidemiologist uses data to provide information to community partners about prevalent diseases in South Dakota. Also, each Program Manager or epidemiologist publishes an annual statistical report and the HIV Surveillance Coordinator assists with the development of the Epidemiological Profile (published every 4 to 5 years) for the Office of Disease Prevention Services.

3.7 DATA QUALITY

Continuous data validation is conducted within SDEDSS, along with an annual data clean-up completed prior to data submission to CDC.

SDEDSS contains all surveillance data for reportable communicable diseases. Therefore, co-morbidities are easily tracked through SDEDSS. The information about the co-morbidities is accessible to only authorized users, such as DIS, Program Managers, and epidemiologists

For example, the STI Program is linked with HIV/AIDS partner notification activities. Data needed to perform an effective field investigation (demographic, clinical and risk) can be shared between programs. The efforts of DIS to identify contacts of cases can potentially identify new cases of HIV infection. When required, DIS also have an integral role in resolving NIR (no identified risk) investigations. Exchange of information between HIV/AIDS surveillance staff, STD program manager and DIS staff is bilateral and occurs on the state level.

All death certificates are reviewed for reportable disease specific cause of death by the department's Office of Vital Records. When a death certificate shows a cause of death related to a reportable disease, a copy of the death certificate will be forwarded to the surveillance coordinator. Record review of the South Dakota death certificate database is done monthly by the HIV Surveillance Program Manager.

3.8 DATA RELEASE POLICY

The data release policy follows the South Dakota state law 34-22-12.1 and the release of any data must be approved by the ORP, her designee, and/or State Epidemiologist.

STIs and HIV/AIDS Only: STD and HIV surveillance case data will not be released with cell sizes less than or equal to 5. For example, if HIV data is presented by county, counties with 5 or fewer cases should be represented by <u>&lt;</u>5. Counties with zero (0) cases can be represented as zero (0). Exceptions to the cell size data release will be made only by the approval of the ORP or State Epidemiologist.

4.0 PHYSICAL SECURITY

4.1 HARD COPIES

Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room.
When identifying information is taken from the secured area included on supporting notes, or other 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 term that could easily be associated with a disease.

When accessing SDEDSS during business travel, users must use a State-owned, BIT-supported device and only access from a private, secure room. A secure Citrix application, a state-run VPN, My Apps, or an approved SDEDSS secure portal must be used to ensure encryption. Users must log off SDEDSS and/or Citrix/VPN, and lock the computer when they are not present in the room. Users must not use unsecure, public connections to the internet (e.g. weak or no password access). If possible, access using a State-owned, BIT supported device hotspot. Authorization for Offsite Access to SDEDSS form must be completed prior to accessing SDEDSS from all offsite locations.

If hard copy or digital surveillance information with personal identifiers is taken into the field or private residences, staff must adhere to these security standards.

Prior approval must be obtained from the appropriate Program Manager or epidemiologist when business travel precludes the return of surveillance information with personal identifiers to the secured area by close of business day on the same day. Information with personal identifiers must not be taken to private residences, with rare exceptions.

Under exceptional circumstances, surveillance information with personal identifiers may be taken to private residences without approval if an unforeseen situation were to arise that would make returning to the surveillance office impossible or unsafe. For example, if a worker carrying sensitive information were caught in a sudden heavy snowstorm, driving home instead of returning to the office would be permissible provided the workers supervisor is notified (or an attempt was made to notify the supervisor of the need to return home with the sensitive information). Precautions must be taken at the worker's home to protect the information under such circumstances. All competed, or partially completed, paper case report forms should be transported in a locked satchel or briefcase.

When accessing SDEDSS from home, state users must use a State-owned, BIT-supported device and ensure encryption using the Citrix application or an approved SDEDSS secure portal. Use of SDEDSS must occur in a designated and secure, private room. Users must log off SDEDSS and/or Citrix, and lock the computer, when they are not present in the room. Users must not use unsecure, public connections to the internet (e.g. weak or no password access). If possible, access using a State-owned, BIT supported device hotspot. Authorization for Offsite Access to SDEDSS form must be completed prior to accessing SDEDSS from home. Please see Appendix N.

4.2 CROSSCUTTING OF CONFIDENTIAL DOCUMENTS

Each member of the surveillance staff must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature.

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

All incoming mail is opened by an 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 42-58 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 respective ORP.

4.5 LINE LISTS

Line-lists typically contain the client name, Date of Birth (DOB), status (HIV or TB), 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 so as 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 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 STDS, HIV or AIDS.

Replacement of the following terms associated with STD’s, HIV, and AIDS will be as follows:
900 (HIV) 950 (AIDS) 700 (Syphilis) 300 (GC) 200 (Chlamydia)

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 the course of an investigation.

5.0 ELECTRONIC DATA SECURITY

5.1 ELECTRONIC PROTECTIVE SOFTWARE

Maximum security practice dictates that communicable surveillance data be maintained on a dedicated file server at only one site in each project area where layers of security protections can be provided.

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 requires users to login to gain access to the State's internal network, ensuring continuity of critical Department of Health 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 eHARS and SDEDSS database servers are maintained on a secure LAN drive in the central office. eHARS and the SDEDSS database are stored on state-controlled servers. eHARS is backed up with a SQL Server agent. Full eHARS backups are done nightly with transaction log backups also done nightly. The database has 60 days of transaction log and daily backups on a 13-month retention cycle. Full SDEDSS backups are done nightly with transaction log backups are also done nightly. The database has 60 days of transaction log and daily backups on a 13-month retention cycle.

The LAN server is in a locked room accessible to only the computer systems administrators. eHARS is protected by a password security system and is accessible to only the surveillance coordinator, or designee. SDEDSS security standards meet the established HIPAA standards. Each user is assigned a unique username and password. SDEDSS uses a role-based security environment, which displays only the data the user needs and is authorized to see. SDEDSS login authentication uses a password-based authentication where password hashes are compared against the hashed (SHA) passwords in the database. SDEDSS obtains detailed information on each login attempt including the username, timestamp, server source IP address, and browser user-agent.

5.2 APPROVAL BY ORP FOR ELECTRONIC DATA TRANSFER

Data transfers and methods for data collection must be approved by the respective 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.

Electronic files stored for use by authorized surveillance staff should be encrypted until they are actually needed. If these files are needed outside of the secure area, real time encryption or an equivalent method of protection is required.

This requirement also applies in those situations where surveillance data are obtained electronically from external sources (clinical data management systems and laboratories). Extracts from those systems need to be protected as if they were extracts from the surveillance data system.

Transferring data between States (Interstate Notification) will be done according to National Institute of Standards and Technology (NIST) standards.

Case specific information transferred between the HIV Surveillance Coordinator and the DIS must use land phone lines, regular mail, e-mail that incorporates the use of 900/950 status in place of HIV or AIDS or SDEDSS. Use of fax machines is highly discouraged.

Rarely, there may be the need to transfer surveillance information by fax machine between the surveillance coordinator and the DIS. If a fax machine must be used, it is imperative that the sender call the receiver prior to faxing to assure that the receiver is standing by to receive the fax in order that no unauthorized person obtains access to the information.
Please see Appendix H.

5.3 ENCRYPTION ELECTRONIC DATA

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 respective ORP must not contain identifying information or use terms easily associated with a disease. The terms HIV or AIDS, STD, TB or any distinguishable disease identification and/or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/ or recipient address and label.
The intent of this requirement is to eliminate the possibility that a third party may identify a person as being a member of a disease risk factor group. For example, when trying to locate an HIV-infected person during a “No Identified Risk” (NIR) investigation or interview, do not send letters or leave business cards or voice messages at the person’s residence that include any terminology that could be associated with HIV or AIDS.

Similarly, if a third party calls the telephone number listed on a card or letter that party should not be able to determine by a phone greeting that it is an HIV/AIDS surveillance unit or any other disease specific surveillance unit.

If secure fax or encrypted e-mail transmissions are used at all (although CDC strongly discourages their use), care must be taken to avoid linking disease or risk factor status with identifiable information about a person; terms such as HIV, AIDS, STD, will be replaced with their respective disease code (900, 950, 200/300,700) when code has been assigned.

CDC’s policy requires encryption when any moderately or highly critical information or any limited access/proprietary information is to be transmitted to or from CDC either electronically or physically. All data that meet these criteria must be encrypted using the Advanced Encryption Standard (AES). Please see Appendix G.
Currently, CDC requires that this category of electronic data be sent via its Secure Access Management Services (SAMS) portal. The SAMS uses technology to create a Secure Sockets Layer (SSL) or encrypted tunnel through which data are transmitted.

5.4 LAPTOPS AND PORTABLE DEVICES

Laptops, tablets, and other portable devices that receive or store surveillance information with personal identifiers must incorporate the use of encryption software, although storing data on any external storage device or any portable/removable hard drive is strongly discouraged.

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. Laptop or other devices that receive STD or HIV data will use a secure wireless network.

All removable or external storage devices containing surveillance information that contains personal identifiers must:

1. Include only the minimum amount of information necessary to accomplish assigned tasks as determined by the HIV Surveillance Coordinator;

2. Be encrypted or stored under lock and key when not in use; and

3. With the exception of devices used for backups, devices should be sanitized immediately following a given task.

4. External storage devices include but are not limited to diskettes, CD-ROMS, USB port flash drives (memory sticks), zip disks, tapes, smart cards, and removable hard drives.

5.5 DESTRUCTION OF INFORMATION ON HARD COPIES AND ELECTRONIC DEVICES

Acceptable methods of sanitizing discs or other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse or physically destroyed. Physical destruction would include the device, not just the plastic case around the device.

If the machine is 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.

ANNUAL REVIEW AND REVISION HISTORY

Date	*Action*	*Section*	*Reviewer*
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 Shmulski; 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 Shmulski, 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*	*Entire Document*	*Nicholas Hill Surveillance Program Manager* *Mark Zickrick BIT* *Christine Olson HIV Surveillance Program Manager*

	Added Appendix N Page 60 Appendix O Page 59 (Requirement 33, 34, & 35)		
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/nchhstp/programintegration/data-security.htm

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 PS18-1802** 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 PS18-1802 year 5 extension period 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 PS18-1802**. 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 PS18-1802**. 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
Beth Dokken	Division Director	South Dakota Department of Health, Family and Community Health

Applicant/Jurisdiction Name South Dakota Department of Health	Grant/Cooperative Agreement Number NU62PS924534
Signature Overall Responsible Party (ORP) Beth Dokken	Date 4/14/2023
Signature Authorized Business Official Darcy McGuigan	Date 3/31/2023
Signature Principal Investigator (s)	Date 3/31/2023

APPENDIX B – CONFIDENTIALITY OATH

All Department of Health, Division of Family and Community Health or Epidemiology, Surveillance, and Informatics Center, 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-13, revised: September 6, 2022, Title: HIPAA- Business Associates, 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- 13, revised: September 6, 2022, Title: HIPAA –Business Associates.
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.~~,~~
10. I will not discuss any identifying information except in the performance of job-related duties and will be mindful that these discussions do not occur in public areas such as hallways, elevators, restrooms, lunchrooms, or other public 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. Personnel who are authorized to work with surveillance information with identifiers will be supplied a copy of the Data Security and Confidentiality Guidelines. I have reviewed, understood and had opportunity to seek clarification regarding all content provided in this document and how it applies to my authorized use of data and information for my position.
13. I will report activities by any other 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.

____   ____________________

Director, Division of Family and Community Health   Date

Overall Responsible Party (ORP)

____

State Epidemiologist Date
Overall Responsible Party (ORP)

Revised November, 2022

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

STATEMENT NO. GA-13
TITLE: HIPAA – Business Associates
ISSUED: November 1, 2006
REVISED: September 6, 2022

HIPAA privacy rules identify a category of business relationship called a "business associate". This policy specifies when the Department of Health (DOH) may disclose an individual's protected health information (PHI) to a business associate of the DOH and specifies provisions that shall be incorporated into all contracts between the DOH and a business associate.

A. Definitions

1. *Business Associate:* "Business Associate" means (per 45 CFR §160.103):
   (a) With respect to the DOH, a person who:
   1. On behalf of the DOH, but other than in the capacity of a DOH employee, performs or assists in the performance of:
      a. A function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing benefit management, practice management, and repricing; or;
      b. Any other function or activity regulated by federal regulations at 45 CFR Subtitle A, Subchapter C; or;
   2. Provides, other than in the capacity of a DOH employee, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the DOH, or for an organized health care arrangement in which the DOH participates, where the provision of the service involves the disclosure of individually identifiable health information from the DOH, or from another business associate of the DOH, to the person.

   (b) A covered entity participating in activities or providing services as described in (a)(1) or (a)(2) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
   (c) A covered entity may be a business associate of another covered entity.
   (d) The following are NOT business associates or business associate relationships: (1) DOH employees, offices, and programs; (2) medical providers providing treatment to individuals; (3) enrollment or eligibility determinations involving DOH clients between government agencies; (4) payment relationships, such as when the DOH is paying medical providers, child care providers, managed care organizations, or other entities for services to DOH clients or participants when the entity is providing its own normal services that are not on behalf of the DOH; (5) when an individual's PHI is disclosed based solely on an individual's authorization; (6) when an individual's PHI is not being

disclosed by, or created for, the DOH; and (7) when the only information being disclosed is information that is de-identified.

2. *Protected Health Information:* Individually identifiable health information, including demographic information, such as age, address, and account numbers, and information that relates to a program participant's past, present, or future physical or mental health or condition or related health care services.

B. Policy

1. General

(i) The DOH may disclose an individual's PHI to a business associate and may allow a business associate to create or receive an individual's PHI on behalf of the DOH, if the business associate has first entered into a contract with the DOH which incorporates this policy into the terms of such contract.

(ii) A business associate relationship is formed only if PHI is to be used, created, or disclosed in the relationship.

(iii) If a contractor or business partner is a "business associate", the contract that defines the contractual relationships remains subject to all federal and state laws and policies governing the contractual relationship, in addition to the requirements of this policy which are incorporated into such contract as additional contract provisions.

2. Requirements Applicable to Business Associates a. All business associates shall:

a. Not use or further disclose PHI other than as specifically permitted or required by the contract or as required by law;

b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the contract;

c. Report to the DOH any use or disclosure not allowed by the contract of which the business associate becomes aware;

d. Ensure that any agents or subcontractors to whom it provides PHI agrees to the same restrictions and conditions that apply to the business associate under the contract;

e. Make PHI available to the individual in accordance with *Administrative Policy Statement No. 12*;

f. Makes its internal practices, books, and records relating to the use and disclosure of PHI available to the DOH and to the U.S. Department of Health and Human Services for the purpose of determining the DOH's compliance with federal requirements; and

g. At termination of the contract, if reasonably feasible, return or destroy all PHI that the business associate still maintains in any form, and keep no copies thereof. If not feasible, the business associate will continue to protect the information.

3. The DOH may authorize termination of the contract if the DOH determines that the business associate has violated a material term of the contract.

(i) If the business associate of the DOH is another governmental entity:

a. The DOH may enter into a memorandum of understanding (federal) or a joint powers agreement (state) rather than a contract with the business associate if the memorandum of understanding or joint powers agreement contains terms covering all objectives of 2.a., above, of this policy;

b. The memorandum or agreement does not need to contain specific provisions required under 2.a., above, if other law or regulations contain requirements applicable to the business associate that accomplish the same objective.

4. If a business associate is required by law to perform a function or activity on behalf of the DOH, or to provide a service to the DOH, the DOH may disclose PHI to the business associate to the extent necessary to enable compliance with the legal requirements, without a written contract or agreement, if:

a. The DOH attempts in good faith to obtain satisfactory assurances from the business associate that the business associate will protect health information to the extent specified in 2.a., above; and

b. If such attempt fails, the DOH documents the attempt and the reasons such assurances cannot be obtained.

5. Other requirements: If specifically authorized in the written contract or agreement between the DOH and the business associate, the business associate may:

a. Use information it receives in its capacity as a business associate to the DOH, if necessary;

6. Disclose information is receives in its capacity as a business associate if:
   (i) The disclosure is required by law; or
   (ii) The business associate receives assurances from the person to whom the information is disclosed that:

      a. It will be held or disclosed further only as required by law or for the purposes to which it was disclosed to such person; and
      b. The person will notify the business associate of any known instances in which the confidentiality of the information has been breached.

7. Responsibilities of the DOH in Business Associate Relationships
   (i) The DOH's responsibilities in business associate relationships include, but are not limited to, the following:
      a. Receiving and logging an individual's complaint regarding the uses and disclosures of PHI by the business associate or the business associate relationship;
      b. Receiving and logging reports from the business associate of possible violations of the business associate contracts;
      c. Implementation of corrective action plans, as needed; and
      d. Mitigation, if necessary, of known violations up to and including contract termination.
8. The DOH will provide business associates with this policy or any subsequent modifications, and may provide consultation to business associates as needed on how to comply with contract requirements and this policy regarding PHI.

STATEMENT NO. GA-12
TITLE: HIPAA – General Provisions
ISSUED: November 17, 2018; revised September 6, 2022

The purpose of this policy is to set the Department of Health (DOH) policy regarding compliance with the Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164 (HIPAA).

A. Definitions
Program Participant: A person participating or enrolled in one of the DOH's programs that provides health-related services and collects and maintains protected health information.
Protected Health Information (PHI): Individually identifiable health information, including demographic information, such as age, address, and account numbers, and information that relates to a program participant's past, present, or future physical or mental health condition or related health care services.

B. Notice of Privacy Practices (45 CFR §164.520)
The DOH will develop and maintain a Notice of Privacy Practices and provide such notice to all program participants, as required by law. The acknowledgement form signed by program participants shall be retained by the DOH according to state retention policies for a period of six years.

C. Right to Access, Inspect and Copy PHI (45 CFR §164.524)
Upon receipt of a written request, the DOH will provide a program participant with access to his/her PHI maintained by the DOH, as required by law, and will offer the program participant a review process

when certain requests are denied. When access is provided, a program participant will be allowed to obtain a copy of the information requested. However, the DOH may charge the program participant for the reasonable costs associated with providing such access in accordance with Administrative Policy Statement No. GA-22.

D. Right to Accounting of Disclosure of PHI (45 CFR §164.528)

Upon receipt of a written request, the DOH will provide a program participant with an accounting of the DOH's disclosure of the program participant's PHI, as required by law. If the DOH is unable to provide the accounting within the required time period, it will provide a written statement of the reasons for the delay and the date the accounting will be made available. Disclosures made for treatment, payment, or health care operations are not required to be logged or disclosed.

The DOH may charge a program participant for the reasonable costs associated with providing such disclosure in accordance with Administrative Policy Statement No. GA-22. The DOH may suspend a program participant's right to an accounting of disclosures under limited circumstances, as authorized by law.

E. Right to Amendment of PHI (45 CFR §164.526)

Upon receipt of a written request, the DOH will amend PHI maintained by the DOH, as required by law. The DOH may deny certain requests for amendments, but will properly notify the program participant in the event of a denial and explain how the program participant may respond to a denial.

F. Right to Restrict Use and Disclosure of PHI (45 CFR §164.522)

Upon receipt of a written request, the DOH will restrict its use and disclosures of a program participant's PHI, as required by law. However, the DOH is not required to agree to all restrictions. If the DOH agrees to a restriction, it may later terminate its agreement under limited conditions.

G. Right to Confidential Communications (45 CFR §164.522)

A program participant (or personal representative) may ask that the DOH take reasonable steps to ensure that communications with the program participant remains confidential. This can be achieved by contact through an alternate means or location (i.e., alternate phone number or address). The DOH can accept or deny requests based on the feasibility of each individual request, and may later terminate the request in limited circumstances.

H. Complaints (45 CFR §160.530)

The DOH will take all reasonable and good faith efforts to maintain the strict rules relative to HIPAA to maintain the privacy of a program participant's PHI. A program participant (or personal representative) who feels his/her privacy rights under HIPAA have been violated by the DOH may file a formal complaint with the DOH Compliance Officer. Any DOH employee who receives a complaint will report the incident to the DOH Compliance Officer. A program participant may also file a complaint directly with the federal Office for Civil Rights by calling 866-627-7748 or visiting www.hhs.gov/ocr/hipaa.

I. Confidentiality (45 CFR §160.530)

Information obtained by DOH employees about individuals receiving services through any DOH programs may not be disclosed without the individual's consent, except as authorized by HIPAA, by law, or as permitted by DOH policy. Information may be disclosed in de-identified form that does not identify the individual. All DOH employees shall sign a confidentiality agreement acknowledging they have received training on HIPAA policies and procedures and that they will adhere to the guidelines set out related to confidentiality of a program participant's PHI. The signed confidentiality agreement shall be filed with the employee's supervisor.

J. De-Identification of PHI (45 CFR §164.514)

The DOH may use or disclose PHI if it has applied generally accepted statistical and scientific principles and methods for rendering information not individually identifiable and document there is a very small risk that the information could be used to identify the program participant. The DOH program deidentifying the information will have a means to re-identify the information should they need it.

K. Marketing (45 CFR §164.514)

The DOH will adhere to all requirements that allow PHI to be used or disclosed without authorization. The DOH will also give program a participant the opportunity to opt-out of any or all marketing communications. Marketing is defined as any communications about a product or service, the purpose of which is to encourage recipients of the communication to purchase or use the product or service. This provision excludes communications made by a covered entity (health care provider) as part of the treatment of a program participant, or made by the DOH in the course of managing an individual's treatment.

L. Minimum Necessary (45 CFR §164.514)

The DOH will ensure that all persons providing DOH services have access only to the minimum necessary amount and type of PHI needed to perform the functions for their specific job duties.

M. Research (45 CFR §164.512)

The DOH will adhere to the requirements related to research as defined in the HIPAA regulations. The DOH will be required to obtain each program participant's voluntary and informed authorization before using or disclosing PHI for research. The program participant (or personal representative) will also have the right to revoke his or her authorization at any time by providing the proper written notice. Deidentified or aggregate information will be used whenever possible to limit the exposure of PHI (see Section H. above). Research is defined as a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge with the primary purpose of protecting the health of the population through such activities as disease surveillance, prevention, and control.

N. Sanctions

Any DOH employee who is found in violation of this policy will be subject to the following sanctions depending upon the severity of the violation:

A verbal warning of the violation, no response required;
A written warning of the minor violation, no response required;
A formal written warning of a serious violation, corrective action plan required; or
Termination of employment for blatant violations.
Any disciplinary action taken will be done in accordance with ARSD 55:10:07.

APPENDIX E – SDDOH FAMILY AND COMMUNITY HEALTH STAFF DIRECTORY

A directory including addresses, phone numbers, and email addresses of Central Office staff, Disease Intervention Specialists, Regional managers can be viewed here: https://intranetdoh.sd.gov/Documents/FamilyCommunityHealth_Directory.pdf

Family and Community Health- Beth Dokken, Director, 605-773-4780

Administrator of Office of Disease Prevention and Health Promotion: Kiley Hump 605-773-5610

Infectious Disease Director & Deputy Administrator of Office of Disease Prevention and Health Promotion: Angela Cascio 605-773-4900

- Disease Prevention Program Director/HAI and AR Program Manager: Lori Koenecke, 605-773-4672
- Northeast/Central Regional Supervisor: Greta Thorpe, 605-626-2403
- Western Regional Supervisor: Summer Radke, 605-394-2519
- Southeast Regional Supervisor: Brenda Hansen, 605-367-4610
- HIV/AIDS Prevention Coordinator: Sarah Zaiser, 605-367-7202
- Ryan White Program Coordinator: Deborah Rumrill, 605-367-4795
- STI Program Coordinator: Kacee Redden, 605-773-4794
- TB Program Coordinator: Kristin Rounds, 605-773-4784

Epidemiology- Dr. Josh Clayton, State Epidemiologist, 605-773-2795

- Info. Surveillance Lead: John Shmulsky, 605-773-
- SAS Developer: Stephanie Guggisberg, 763-923-5142
- PowerBI Analyst: Himatheja Veluri, 505-369-8666
- Blood Lead Epidemiologist: Rose Belany, 605-295-7870
- EIS Officer: Hayden Hedman, 605-773-2741
- ODA Syndromic Epidemiologist: Erin Kinder, 605-367-7079
- Deputy State Epidemiologist: Dustin Ortbahn, 605-773-3914
    - Influenza Epidemiologist: Vickie Horan, 605-773-6195
    - Enteric Epidemiologist: Jessica Williams, 605-367-5956
    - Vector Borne Epidemiologist: Anita Bharadwaja, 605-367-7103
    - Viral Hep/HIV/STD/TB/HAI Epi, Nato Tarkhashvili, 605-773-2709
    - Vaccine Preventable Disease Epidemiologist: Sara Bowman, 605-394-2423
    - Informatic Epidemiologist: Chelsea McMullen, 203-927-9177
    - Healthcare Epidemiologist Acting Tribal Health Epi: Liz Roden, 605-280-0531
    - Viral Hep/HIV/STD/TB/HAI Epi: Fabricia Latterell, 605-626-2504
    - Education Epidemiologist: Lexi Ortiz, 605-295-7859
    - Informatics Epidemiologist: Anne Bergman, 605-295-7997
    - Case&Contact Management Epidemiologist: Hannah Parsons, 605-773-3041
        - Public Health Associate: Zoe Rothberg, 605-367-7129
        - Epidemiology Assistant: Anthony Diab 605-295-4290

- Director ID Info: Elizabeth Burdick, 605-773-5710
    - Informatics Assistant: Anthony Diab, 605-295-4290
    - Lab Interface Specialist: Amanuel Petros, 605-773-5712
    - GIS Analyst: Jeff Earl, 605-773-5713
    - Data Scientist: Ruth Bidwell, 605-295-7873
- DIS:
    - Stephanie Harris, 605-773-8224
    - Molly Hausmann, 605-773-8224
    - Nicole Hofeldt, 605-773-5348
    - Jannette Norum, 605-773-2538
    - Tiffany Masteller, 605-951-9121
    - Stephanie Mais, 605-951-9165
    - Katie Gillaspie, 605-394-1995
    - Summer Gillaspie, 605-394-2289
    - Amanda Headley, 605-394-6041
    - Mary Grace lee, 605-394-2281
    - Anastasia Nemec, 605-394-2290
    - Ashley Klatt, 605-882-5097
    - Meghan Marx, 605-882-5037
    - Marcy Harder, 605-626-2373
    - Sadie Hedges, 605-295-7854
    - Robbie Burandt, 605-367-5365
    - Tim Gacke, 605-367-5456
    - Ally Gross, 650-367-7718
    - Sam Hill, 605-367-5396
    - Kelly Kabala, 605-367-5362
    - Courtney Voss, 605-367-716
    - Michael Zielenski, 605-367-5439
    - Angela Eide, 605-995-8051
    - Sarah Ashley, 605-295-4281
    - KathrynJo McGinnis, 605-224-6287
    - Danielle Radel, 605-280-1888
    - Rachel Lohr, 605-295-1211
    - Morgan Pleuger, 605-940-2891
    - Amanda Holland, 605-626-2504
    - Deanna Harber, 605-626-2373
    - Lexi Frank, 605-367-5370

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

Active and inactive users located at M:\DOH\Disease Prevention\ODP\EPI Manual\Data Security and Confidentiality

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 Publication 197

November 26, 2001

Name of Standard: Advanced Encryption Standard (AES) (FIPS PUB 197).
Category of Standard: Computer Security Standard, Cryptography.
Explanation: The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.
Approving Authority: Secretary of Commerce.
Maintenance Agency: Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

APPENDIX H – GUIDELINES FOR THE USE OF FACSIMILE MACHINES

The facsimile machine must be inside a locked and secure area with limited access. If secure faxes are used, care must be taken to avoid linking disease or risk factor status with identifiable information about a person. Disease codes should be used rather than disease names or abbreviations. TB Control Program records will be an exception and therefore will be allowed to be faxed with disease name and risk factor information; however, these records will only be faxed to licensed medical providers or state, city or county health departments. General Epi Program records will be an exception and therefore will be allowed to be faxed with disease name and risk factor information; however, these records will only be faxed to state, city or county health departments.

The fax machine located in the DOH is located in a secure building, in a lockable office/room, with limited staff access. Staff have designated inboxes where faxes can be delivered.

Every effort should be used to prevent misdialing and outdated fax numbers. When possible, pre-programed destination numbers are used and periodically checked for accuracy. When manually entering a fax number, double check that the number is correct before sending. For destinations receiving regular faxes from our office, remind them to let us know if fax numbers change.

Staff are trained on faxing policies, and a reminder of how proper faxes are sent is posted near the fax machine. A cover sheet is to be used for every outgoing fax. The cover sheet should contain contact information of the recipient and sender, as well as a 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/STD/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/STD/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

5 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/STD/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

5 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/STD/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/STD/TB/EPI/BT/Immunization information and data by personnel outside the HIV/VH/STD/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/STD/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?
5 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/STD/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/STD/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/STD/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/STD/TB/EPI/BT/Immunization analysis data sets whenever possible?

STANDARD 5.2

□ Yes □ No	In your program, do transfers of HIV/VH/STD/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?
5 Yes □ No	When individual-level HIV/VH/STD/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/STD/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/STD/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

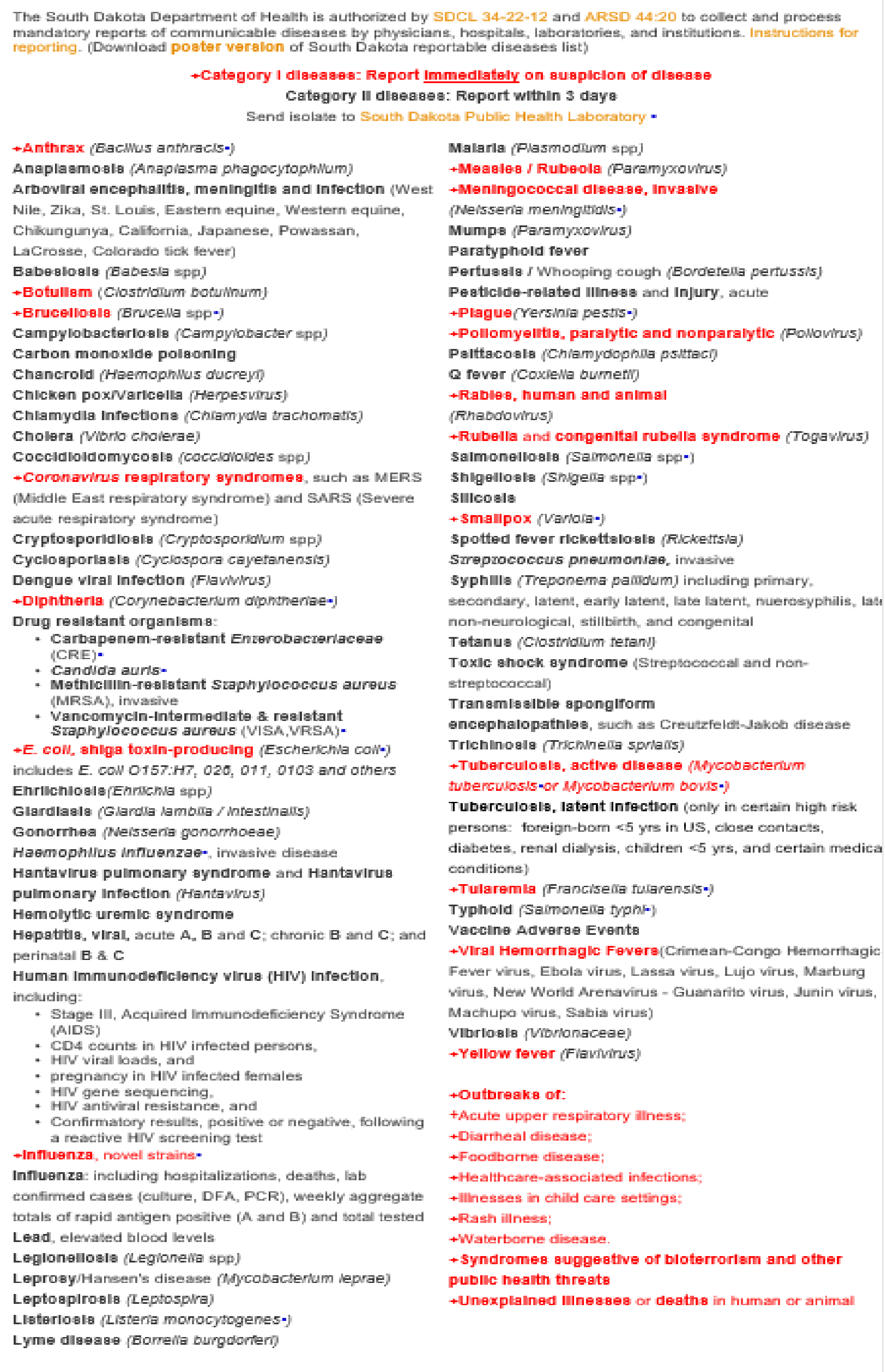
	separated from the laptop and held securely when not in use. □ The decryption key is kept some place other than on the device.
□ Yes □ No	Do the methods employed for sanitizing a storage device ensure that the information cannot retrieved using “undelete” or other data retrieval software?
□ Yes □ No	Does the program have policies or procedures to ensure that all removable or external storage devices containing HIV/VH/STD/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

(Effective January 2019)



The South Dakota Department of Health is authorized by SDCL 34-22-12 and ARSD 44:20 to collect and process mandatory reports of communicable diseases by physicians, hospitals, laboratories, and institutions. Instructions for reporting. (Download **poster version** of South Dakota reportable diseases list)

+Category I diseases: Report Immediately on suspicion of disease

Category II diseases: Report within 3 days

Send isolate to South Dakota Public Health Laboratory ▪

+Anthrax *(Bacillus anthracis▪)*

Anaplasmosis *(Anaplasma phagocytophilum)*

Arboviral encephalitis, meningitis and infection (West Nile, Zika, St. Louis, Eastern equine, Western equine, Chikungunya, California, Japanese, Powassan, LaCrosse, Colorado tick fever)

Babesiosis *(Babesia* spp*)*

+Botulism (*Clostridium botulinum)*

+Brucellosis *(Brucella* spp▪*)*

Campylobacteriosis *(Campylobacter* spp*)*

Carbon monoxide poisoning

Chancroid *(Haemophilus ducreyi)*

Chicken pox/Varicella *(Herpesvirus)*

Chlamydia infections *(Chlamydia trachomatis)*

Cholera *(Vibrio cholerae)*

Coccidioidomycosis *(coccidioides* spp*)*

+Coronavirus respiratory syndromes, such as MERS (Middle East respiratory syndrome) and SARS (Severe acute respiratory syndrome)

Cryptosporidiosis *(Cryptosporidium* spp*)*

Cyclosporiasis *(Cyclospora cayetanensis)*

Dengue viral infection *(Flavivirus)*

+Diphtheria *(Corynebacterium diphtheriae▪)*

Drug resistant organisms:

- **Carbapenem-resistant** ***Enterobacteriaceae*** (CRE)▪
- ***Candida auris***▪
- **Methicillin-resistant** ***Staphylococcus aureus*** (MRSA), invasive
- **Vancomycin-intermediate & resistant** ***Staphylococcus aureus*** (VISA,VRSA)▪

+*E. coli*, shiga toxin-producing *(Escherichia coli▪)* includes *E. coli O157:H7, 026, 011, 0103 and others*

Ehrlichiosis*(Ehrlichia* spp*)*

Giardiasis *(Giardia lambila / intestinalis)*

Gonorrhea *(Neisseria gonorrhoeae)*

Haemophilus influenzae▪, invasive disease

Hantavirus pulmonary syndrome and **Hantavirus pulmonary infection** *(Hantavirus)*

Hemolytic uremic syndrome

Hepatitis, viral, acute A, B and C; chronic B and C; and perinatal B & C

Human immunodeficiency virus (HIV) infection, including:

- Stage III, Acquired Immunodeficiency Syndrome (AIDS)
- CD4 counts in HIV infected persons,
- HIV viral loads, and
- pregnancy in HIV infected females
- HIV gene sequencing,
- HIV antiviral resistance, and
- 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, elevated 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)*

+Meningococcal disease, invasive *(Neisseria meningitidis▪)*

Mumps *(Paramyxovirus)*

Paratyphoid fever

Pertussis / Whooping cough *(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

+Smallpox *(Variola▪)*

Spotted fever rickettsiosis *(Rickettsia)*

Streptococcus pneumoniae**,** invasive

Syphilis *(Treponema pallidum)* including primary, secondary, latent, early latent, late latent, nuerosyphilis, lat 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 sprialis)*

+Tuberculosis, active disease *(Mycobacterium tuberculosis▪or Mycobacterium bovis▪)*

Tuberculosis, latent infection (only in certain high risk persons: foreign-born <5 yrs in US, close contacts, diabetes, renal dialysis, children <5 yrs, and certain medica conditions)

+Tularemia *(Francisella tularensis▪)*

Typhoid *(Salmonella typhi▪)*

Vaccine Adverse Events

+Viral Hemorrhagic Fevers(Crimean-Congo Hemorrhagic Fever virus, Ebola virus, Lassa virus, Lujo virus, Marburg virus, New World Arenavirus - 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 settings;

+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:	

<u>Section 1: Initial Report</u>
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 or ☐ No

Did a breach in confidentiality occur? ☐ Yes or ☐ No

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

If unknown, please explain why unknown?

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

<u>Section 3: Follow-up Report (To be completed by the Administrator of ODPHP.)</u>

Were any disciplinary actions or corrective actions taken to prevent the breach from occurring again?
☐ Yes or ☐ 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.

<u>Section 4: Final Signatures</u>	
Signature: **(when appropriate)** (electronic accepted) ***Infectious Disease Director***	**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 e-mail to their direct supervisor and respective Program Manager (PM) within 24 hours of the incident. If the PM is not available, then the Infectious Disease Director of the Office of Disease Prevention and Health Promotion (ODPHP) is notified via e-mail.
3. The staff person, contractor, or IT person who reported the suspected breach must receive an e-mail confirmation from the PM 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 Infectious Disease Director of the ODPHP.
4. The PM, Infectious Disease Director, and/or respective ORP will review the initial Breach Report and make a recommendation to the respective ORP for closing out the report when sufficient and reasonable information confirms that a breach has not occurred.
5. The PM will notify the Infectious Disease Director and respective 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 PM has received the breach report, the PM will inform the Infectious Disease Director and/or respective ORP of the suspected breach.
2. The Security Team (Infectious Disease Director, respective ORP, PM) 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 respective 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 ODPHP 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 ODPHP 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:

- 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.
- 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.
- 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 PM will submit a follow-up report via e-mail to both the Infectious disease Director and the respective ORP on a monthly basis. 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.	On a monthly basis, the Infectious Disease Director and the respective 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 PM 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 of this would be: 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 actually 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 actually 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 Program Manager located in the central office responsible for surveillance area, (i.e., Epi, TB, STD, etc.) and to the Administrator of Disease Prevention and Health Promotion and respective ORP(s). Please see Appendix E.

Section 2: Closing Report

This section will be completed with the appropriate central office program manager. They may consult with the person's involved in the incident, their management, the Administrator of the ODPHP and 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.

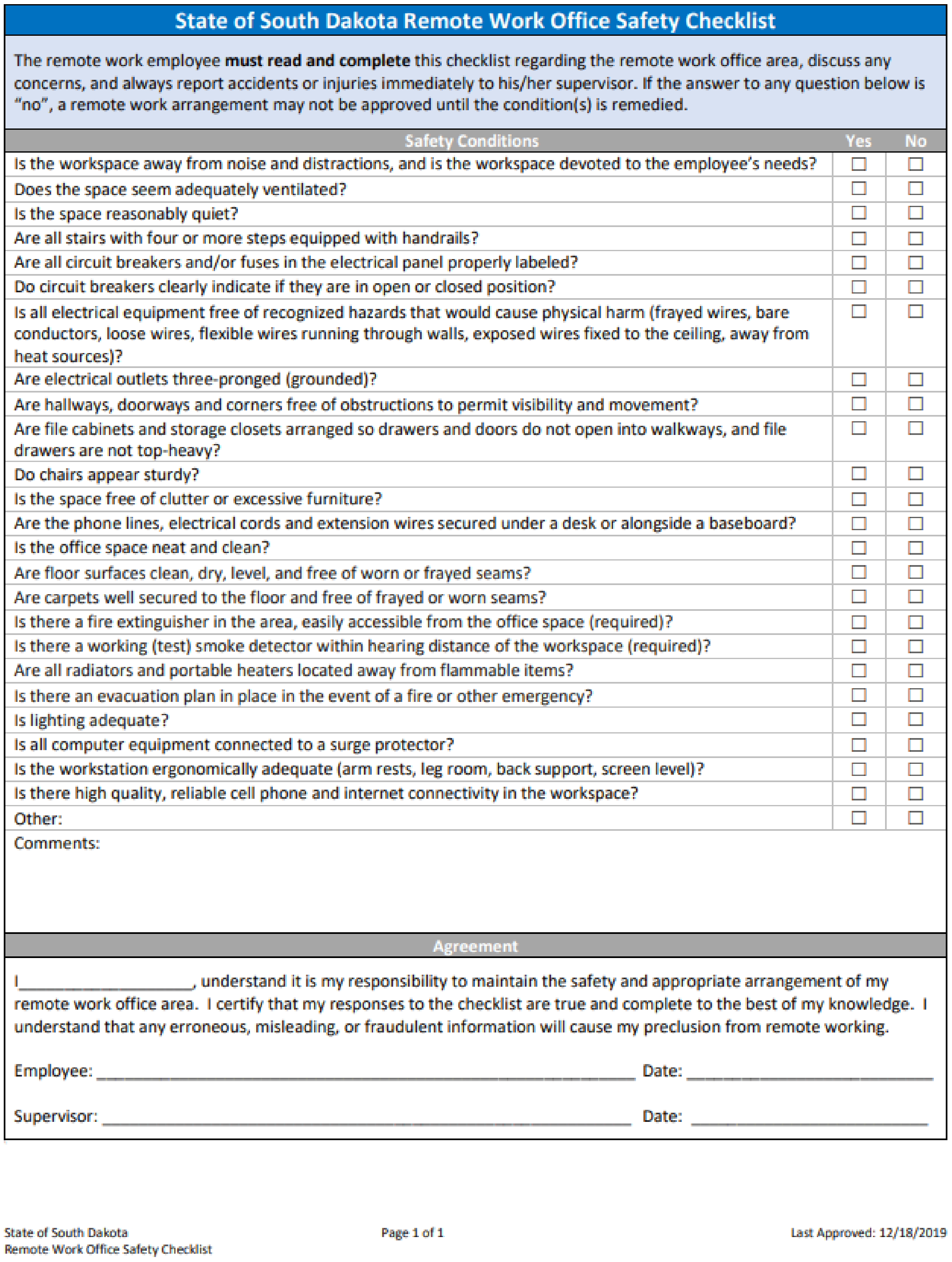
Section 3: Follow Up Report

This section to be completed by the Administrator of the ODPHP or their designee at the central office in Pierre, 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 and Administrator of the Office of Disease Prevention and Health Promotion 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: ____________________

State of South Dakota
Remote Work Office Safety Checklist

Page 1 of 1

Last Approved: 12/18/2019

APPENDIX N – AUTHORIZATION FOR OFFSITE ACCESS TO SDEDSS

The respective 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 define the roles for all persons who are authorized to access what specific information and, for those staff outside the surveillance unit, what standard procedures or methods will be used when access is determined to be 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 staff who are authorized to access surveillance data must be responsible for reporting suspected security breaches. Training of nonsurveillance staff must also include this directive. (1.5)

___ Requirement 8: A breach of confidentiality must be immediately investigated to assess causes and implement remedies. (1.5)

___ Requirement 9: A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. CDC may be able to assist the surveillance unit dealing with the breach. In consultation with appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies. (1.5)

___ Requirement 10: Every individual with access to surveillance data must attend security training annually. The date of the original training must be documented in the employee's personnel file. IT staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc. (1.6)

___ Requirement 11: All authorized staff must annually sign a confidentiality statement. Newly hired staff must sign a confidentiality statement before access to surveillance data is authorized. The new employee or newly authorized staff must show the signed confidentiality statement to the grantor of passwords and keys before passwords and keys are assigned. This statement must indicate that the employee understands and agrees that surveillance information or data will not be released to any individual not granted access by the ORP. The original statement must be held in the employee's personnel file and a copy given to the employee. (1.7)

___ Requirement 12: 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 organization's information security policies and procedures. All staff who are authorized to access surveillance data must be responsible for challenging those who are not authorized to access surveillance data. (1.8)

__ Requirement 13: All staff who are authorized to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold. (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 (e.g. Voltage). (1.8)

___ Requirement 15: Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names, an Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval depending on the numbers and types 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 staff 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 outline procedures for handling incoming mail to and outgoing mail from the surveillance unit. The amount and sensitivity of information contained in any one piece of mail must be kept to a minimum. (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: information 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: *https://intranetdoh.sd.gov/Documents/HIPAAProcedureManual.pdf*

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 M: drive (central office) or X: drive (field office). 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