



SOUTH DAKOTA  
DEPARTMENT OF HEALTH

HIV Confidentiality and Security Training Manual

Issued: May 6, 2006

Revised: February 6, 2009

Reviewed: February 23, 2011

Revised September 22, 2011

*CDC Security and Confidentiality Certification April 21, 2009*

Supporting Documents can be found at:

<http://www.cdc.gov/hiv/topics/surveillance/resources/guidelines/guidance/index.htm>

## Contents

Policies.....	3
Responsibilities.....	8
Training.....	10
Physical Security.....	10
Data Security.....	12
Data Movement.....	12
Sending Data to CDC.....	15
Transferring Data Between Sites.....	15
Access Control.....	15
Security Breaches.....	17
Laptops and Portable Devices.....	18
Removable and External Storage Devices.....	18
Approval Signatures.....	19
<b>Attachments</b>	
A. South Dakota Security and Confidentiality Requirement Check List.....	20
B. South Dakota Confidentiality Oath.....	26
C. South Dakota Codified Laws.....	27
D. South Dakota Admin Policies and Procedures Statement 25.....	29
E. ORP Certification.....	32
F. Table 1 HIV/AIDS Data Systems Access Overview.....	33
G. Federal Encryption Standards.....	35

**South Dakota Department of Health**  
HIV/AIDS Surveillance Program  
Confidentiality and Security Manual

May 6, 2006

Revised February 6, 2009

Reviewed February 23, 2011

**Policies**

1. This confidentiality and security manual has been established to ensure confidentiality of Human Immunodeficiency Virus (HIV) surveillance data. South Dakota state law 34-22-12 required HIV and AIDS cases to be reported 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 17, 2008, Title: HIPAA – General Provisions. Please see Attachments C and D.

National program requirements to protect HIV 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) <sup>1</sup>.

2. As part of the program requirements, the Director of the Division of Health and Medical Services, Colleen Winter, is designated as the Overall Responsible Party (ORP) for HIV surveillance. The ORP has the responsibility for the security of the HIV surveillance system and will annually certify, using the “Security and Confidentiality Program Requirement Checklist,” that all program requirements established by CDC are being followed.

Only DOH personnel who have a need-to-know will have access to HIV surveillance data with identifiers. The surveillance unit consists of the ORP, the Administrator of the Office of Disease Prevention, the HIV Surveillance Coordinator, STD Team Lead and DOH SD-EDSS personnel identified as “Super users”, Information System Specialists, Case Management, Reporting Alerting, and Monitoring System (SD-EDSS), Project Manager, and Data Base Administrators. Please see Table 1 (Attachment F).

The HIV Surveillance Coordinator is located in the central office and is Responsible for writing the HIV surveillance grant application, assigning HIV case investigations to the Disease Intervention Specialists (DIS), the central registry, HIV/Acquired Immunodeficiency Syndrome (AIDS) Reporting System (EHARS) database, dissemination of surveillance data, and transferring data to CDC. The DIS are located across the state in field offices and are responsible for case investigations, active case finding, and pediatric exposure follow-up.

<sup>1</sup>Centers for Disease Control and Prevention, Volume III: Security and Confidentiality Guidelines, January 2006.

### **3. Procedure for review of security practice for HIV / AIDS surveillance data.**

- A.) As part of the review and quality improvement procedure, the HIV Surveillance Coordinator will evaluate progress toward meeting CDC program Requirements by assessing the “Security and Confidentiality Program Requirement Checklist” shown as Attachment A on an annual basis.
- B.) When all changes to information systems technology are proposed, the Information System Specialist and “Super Users” are responsible for collaborating with the HIV Surveillance Coordinator to prepare technical solutions. This collaboration will help ensure that in no way the security and confidentiality of the HIV/AIDS surveillance data are electronically compromised.
- C.) Ongoing review of evolving technology to ensure that data remain secure will be performed by the HIV Surveillance Coordinator.

### **4. Data Release Policy**

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 names 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.*

## **5. Public Access to Raw Data**

- A.) The HIV Surveillance Coordinator will publish an annual statistical report and assist with the development of the Epidemiological Profile for the HIV prevention program. 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 3 or fewer cases should be represented by  $\leq 5$ . Exceptions to the cell size data release will be made only by the approval of the ORP.
- B.) Access to HIV surveillance information with identifiers by those who maintain other disease registries (ex. TB, STD) will be limited to program managers in the Office of Disease Prevention 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.
- C.) Access to HIV Surveillance 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.
- D.) 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. 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.
- E.) Line-lists typically contain the client name, Date of Birth (DOB), status (HIV or AIDs), and risk information. Line lists of HIV clients will not be printed or mailed without prior approval from the HIV Surveillance Coordinator. Line lists will be de-identified with numeric ID so as to neither directly nor indirectly identify the contents of the line-list.

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

- F.) No Global Imaging System (GIS) Mapping or reports will be shared outside users defined in the HIV/AIDS Data Systems Access table, except that defined above in Section 5 A.
- G.) Permission to access HIV data in the electronic Maven are role based and therefore strictly restricted to valid users according to Table 1 (Attachment F). Role based user accounts are set up only by Maven "Super-Users" listed in Table 1 (Attachment F). Assignment of any user accounts by Maven "Super-Users" which will have access to HIV data will only occur after the HIV Surveillance Coordinator has given express permission. Maven "Super-Users" will immediately inactivate any user accounts upon request by the HIV Surveillance Coordinator; Maven "Super-Users" will periodically review user accounts to ensure that only valid users remain active.
- H.) Access to HIV patient records will be limited to surveillance activities only by those authorized by the HIV Surveillance Coordinator or ORP.

## **6. Staff Access to Confidential Surveillance Policy**

The security and confidentiality policy will be posted on a state network shared drive X and N where it is accessible by all staff.

## **7. Defined Roles of Persons authorized to access specific Information.**

Please see Table 1 (Attachment F).

## **8. Confidentiality Statement**

- A.) All authorized staff must annually sign a confidentiality statement. Newly hired staff 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. The original statement will be placed in the employee's personnel file and a copy will be given to the employee. Please see Attachment B.
- B.) 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).

- C.) The HIV Surveillance Coordinator will periodically review the SD-EDSS audit logs to assess whether unauthorized HIV data access has occurred. Breach of security and confidentiality pertaining to HIV/AIDS surveillance information may result in suspension or termination based on the severity of the offense. Disciplinary actions are determined by the statewide ORP.
- D.) Access to the public internet or e-mail applications while accessing surveillance information is not allowed.
- E.) Group authenticators (administrators, super users, etc.) will have information system access as explicitly authorized by the ORP or the HIV Surveillance Coordinator.
- F.) Access to identifiable HIV patient data is not allowed except by the HIV Surveillance Coordinator or as authorized for valid surveillance activities.
- G.) Information technology (IT) authorities must obtain approval from the HIV Surveillance Coordinator before granting access or adding users. A log documenting authorized viewers of data will be reviewed periodically by the HIV Surveillance Coordinator.

## **9. Incoming and Outgoing Mail**

- A.) All incoming mail is opened by the Office of Disease Prevention Administrative Assistant. This person is required to sign the department confidentiality statement. The mail is then dispersed to the HIV/AIDS Surveillance Coordinator.
- B.) Senders of confidential information are instructed to address mail to the HIV Surveillance Coordinator. Whenever confidential information is mailed, double envelopes must be used, clearly marked "Confidential".
- C.) Line lists of HIV clients will not be printed or mailed without prior approval from the HIV Surveillance Coordinator. Line lists will be de-identified so as to neither directly nor indirectly identify the contents of the line-list.
- D.) All outgoing mail containing patient identifiers is marked "Confidential", double enveloped, and sent "Return Service Requested".
- E.) No outgoing envelopes have any direct or indirect reference to HIV/AIDS.

## **Responsibilities**

### **10. ORP**

As part of the program requirements, the Director of the Division of Health and Medical Services, Colleen Winter, is designated as the ORP for HIV surveillance. The ORP has the responsibility for the security of the HIV surveillance system and will annually certify that all program requirements established by CDC are being followed. Please see Attachment E.

### **11. Annual review of security policies and procedures**

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 information security policies and procedures and will be required to annually perform the Security and Confidentiality Program Requirement Checklist. Please see Attachment A.

### **12. Delineation of HIV Surveillance Staff Responsibilities.**

Surveillance staff and all persons described in this document who are authorized to access case-specific information have the following general responsibilities pertaining to the security and confidentiality of HIV/AIDS surveillance information.

1. Challenging unauthorized users of HIV/AIDS surveillance data. Authorized users and authorized use of HIV/AIDS surveillance information are defined in section 5 of this manual.
2. Immediately reporting all suspected breaches of confidentiality to the HIV Surveillance Coordinator, the ORP, or the designee of the HIV Surveillance Coordinator or ORP. The ORP or the designee of the ORP will report breaches to the CDC/HICSB/RAET team Leader, Program Consultant, and Epidemiologist.
3. Exercising good judgment in the daily management of HIV/AIDS surveillance information. From time to time, confidentiality and security issues related to HIV/AIDS surveillance data may arise that are not specially addressed in this manual. When these issues arise,

surveillance staff is responsible for notifying the HIV Surveillance Coordinator who can provide the necessary guidance related to these issues.

### **13. Protection of workstation and other devices**

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.

- A.) 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.
- B.) Ideally, only staff with similar roles and authorizations would be permitted in a secure area.
- C.) Incoming telephone calls will be answered with generic identifiers (e.g., "Department of Health", "This is Christine"), without any direct reference to HIV/AIDS, are used when answering all incoming calls. Confidential information is shared over the phone with individuals authorized to access HIV/AIDS surveillance information as listed in Section 5.
- D.) Outgoing calls requesting confidential information to perform routine HIV/AIDS 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 individual with a need-to-know and always use utmost discretion.

## **Training**

### **14. Annual Security Training**

Every individual and access to surveillance data must attend security training annually. The date of 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 device, etc.

Security training is required for all new staff and annually thereafter.

Trainings will vary based on circumstances. For example, one-on-one trainings may take place in the central office where there is one HIV Surveillance staff, but with larger numbers of staff, periodic group training sessions may be more appropriate.

## **Physical Security**

Maximum security practice dictates that HIV/AIDS 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 such as Department of Health DIS field offices that are within the firewall that access the central surveillance server for authorized surveillance activities will access the server through a secured method as required by BIT (e.g. encryption).

The eHARS and Maven database servers are maintained on a secure LAN drive in the central office. eHARS is stored on server ESPR10085. eHARS is backed up with a SQL Server agent. Full eHARS backups are done nightly with transaction log backups every 12 hours. The database has 60 days of transaction log and daily backups with 13 months of monthly back ups.

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, designee, or the STD Team Leader.

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

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 are located.

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

**15. Physical location containing electronic or paper copies**

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

**16. Paper copies**

Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room.

**17. Disposing of Confidential Information**

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.

**18. 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.

### **Data Security**

A remote site is defined as a site that remotely connects to and accesses a centralized database to enter and store surveillance data even though paper forms may be stored locally. The central database is located in a different physical location than the remote site.

### **Data Movement**

- 19. Surveillance information must have personal identifiers removed if taken out of the secured area or accessed from an unsecured area.**

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 HIV or AIDS.

Prior approval must be obtained from the ORP 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. HIV surveillance information with personal identifiers must not be taken to private residences, with rare exceptions. If exceptions occur, they must be documented.

- 20. An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data).**
- 21. 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.**

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. Additionally, those systems within DOH will be held to the same standards as the HIV/AIDS surveillance systems.

## **22. Case-Specific Information Electronically Transmitted.**

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.

The intent of this requirement is to eliminate the possibility that a third party may identify a person as being a member of an HIV risk factor group or HIV infected. 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.

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 HIV or risk factor status with identifiable information about a person. Terms such as HIV or AIDS will be replaced with 900 or 950.

### **23. Identifying taken from secured areas**

When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or head 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 and information that could easily be associated with HIV or AIDS.

Replacement of the following terms associated with HIV or AIDS will be as follows:

900 (HIV)  
950 (AIDS)

The requirement applies to information or data taken from secure areas. It does not refer to data collected from the field and taken to secure areas. While coding of terms associated with HIV/AIDS 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 NIR case during the course of an investigation.

### **24. Private Residences**

Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator.

Under exceptional circumstances, HIV/AIDS surveillance information with personal identifiers may be taken to private residences without approval if an unforeseen situation arises 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 completed, or partially completed, paper case report forms should be transported in a locked satchel or briefcase.

## **25. Planned Business Travel**

Prior approval must be obtained from the surveillance coordinator when planned business travel precludes the return of surveillance information with personal identifiers to the secured areas by the close of business on the same day.

### **Sending Data to CDC**

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 Attachment G.

Currently, CDC requires that this category of electronic data be sent via its Secure Data Network (SDN). The SDN uses digital certificate technology to create a Secure Sockets Layer (SSL) or encrypted tunnel through which data are transmitted.

### **Transferring Data between Sites**

If there is a need to move data within the state or between States data will be encrypted using the criteria described in the previous step, Sending Data to CDC.

### **Access Control**

#### **Local Access**

## **26. Surveillance Information Containing Names for Research Purposes.**

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 **ORP** for direction.

- 27. Access to areas that contain surveillance data can be accessed only during times when authorized surveillance staff are available for escort.**

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

- 28. Access to confidential surveillance information and data by personnel outside the surveillance unit.**

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**.

- 29. Access to surveillance information with identifiers by those who maintain other disease data stores.**

Sexual Transmitted Disease Control program is linked with HIV/AIDS partner notification activities. Data needed to perform an effective field investigation (demographic, clinical and risk) could 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 investigations. Exchange of information between HIV/AIDS surveillance staff, STD program manager and DIS staff is bilateral and occurs on the state level.

In the office of Disease Prevention on an annual basis, names and dates of birth of all tuberculosis and Hepatitis disease cases are matched to names and dates of birth of cases in eHARS. The HIV Surveillance Coordinator conducts the match. If an individual has dual diagnoses, the diagnosis and Report of Verified Case of TB (RVCT) number is noted on the EHARS data base.

All death certificates are reviewed for HIV/AIDS cause of death by the department's Office of Vital Records. When a death certificate shows a cause of death related to HIV/AIDS, a copy of the death certificate will be forwarded to

the surveillance coordinator. Record linkage to the South Dakota death certificate database is done annually by the HIV Surveillance Coordinator.

- 30. Access to surveillance information or data for non-public health purposes, such as litigation discovery, or court order, must be granted only to the extent required by law.**

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 **ORP** approval. Access to surveillance data or information without names may still require **ORP** approval depending on the numbers and types of variables requested and in accordance with data release policies.

### **Security Breaches**

- 31. All staff authorized to access surveillance data are responsible for reporting suspected security breaches. Training of nonsurveillance staff will also include this directive.**
- 32. A breach of confidentiality will be immediately investigated to assess causes and implement remedies.**
- 33. Breach of Confidentiality**

A breach of security involving HIV Surveillance data must be immediately reported to the **ORP**. Documentation of the breach will be maintained by the **ORP** describing the investigation findings and corrective actions taken.

A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the **ORP**. The breach will then be reported to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, Division of HIV/AIDS Prevention (DHAP), as well as CDC Program Consultant and Program Epi by the **ORP**. In consultation with appropriate legal counsel, the **ORP** will determine whether a breach warrants report to law enforcement agencies.

### **Laptops and Portable Devices**

- 34. Laptops and other portable devices (e.g., personal digital assistants [PDAs], other hand-held devices, and tablet personal computers [PCs]) 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 device without removable or external storage components must employ the use of encryption software that meets federal standards. Laptop or other devices that receive HIV data will not use wireless networks.

### **Removable and External Storage Devices**

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



## Attachment A

### South Dakota Department of Health

### Security and Confidentiality Program Requirement Checklist

Person completing form \_\_\_\_\_

Signature \_\_\_\_\_

Date: \_\_\_\_\_

Site: \_\_\_\_\_

#### *Guiding Principles*

- Guiding Principle 1 HIV/AIDS surveillance information and data will be maintained in a physically secure environment. Refer to sections Physical Security and Removable and External Storage Devices.
- Guiding Principle 2 Electronic HIV / AIDS surveillance data will be held in a technically secure environment, with the number of data repositories and individuals permitted access kept to a minimum. Operational security procedures will be implemented and documented to minimize the number of staff that have access to personal identifiers and to minimize the number of locations where personal identifiers are stored. Refer to sections Policies, Training, Data Security, Access Control, Laptops and Portable Devices, and Removable and External Storage Devices.
- Guiding Principle 3 Individual surveillance staff members and persons authorized to access case-specific information will be responsible for protecting confidential HIV/AIDS surveillance information and data. Refer to sections Responsibilities, Training, and Removable and External Storage Devices.
- Guiding Principle 4 Security breaches of HIV / AIDS surveillance information or data will be investigated thoroughly, and sanctions imposed as appropriate. Refer to section Security Breaches.
- Guiding Principle 5 Security practices and written policies will be continuously reviewed, assessed, and as necessary, changed to improve the protection of confidential HIV / AIDS surveillance information and data. Refer to Policies section.

## *Requirements*

(Initial items as read/completed)

- \_\_\_ Requirement 1: Policies must be in writing. (GP-2)
- \_\_\_ Requirement 2: A policy must name the individual who is the Overall Responsible Party (ORP) for the security system. (GP-2)
- \_\_\_ Requirement 3: 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. (GP-5)
- \_\_\_ Requirement 4: Access to and uses of surveillance information or data must be defined in a data release policy. (GP-2)
- \_\_\_ Requirement 5: 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. (GP-2)
- \_\_\_ Requirement 6: 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. (GP-2)
- \_\_\_ Requirement 7: 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. (GP-2)
- \_\_\_ Requirement 8: 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. (GP-2)
- \_\_\_ Requirement 9: 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. (GP-2)
- \_\_\_ Requirement 10: In compliance with CDC's cooperative agreement requirement, the ORP must certify annually that all program requirements are met. (GP-2)

- \_\_\_ Requirement 11: 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. (GP-3)
- \_\_\_ Requirement 12: All staff who are authorized to access surveillance data must be responsible for challenging those who are not authorized to access surveillance data. (GP-3)
- \_\_\_ 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. (GP-3)
- \_\_\_ Requirement 14: Every individual with access to surveillance data must attend security training annually. The date of 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. (GP-3)
- \_\_\_ Requirement 15: 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. (GP-1)
- \_\_\_ Requirement 16: Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room. (GP-1)
- \_\_\_ Requirement 17: 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. (GP-3)
- \_\_\_ Requirement 18: Rooms containing surveillance data must not be easily accessible by window. (GP-1)
- \_\_\_ Requirement 19: Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area. (GP-1)
- \_\_\_ Requirement 20: An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data). (GP-1)

- \_\_\_ Requirement 21: 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. (GP-1)
- \_\_\_ Requirement 22: 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 and AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label. (GP-2)
- \_\_\_ Requirement 23: 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 or AIDS. (GP-1)
- \_\_\_ Requirement 24: Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator. (GP-1)
- \_\_\_ Requirement 25: Prior approval must be obtained from the surveillance coordinator 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. (GP-1)
- \_\_\_ Requirement 26: 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. (GP-1)
- \_\_\_ Requirement 27: 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. (GP-1)

- \_\_\_ Requirement 28: 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. (GP-1)
- \_\_\_ Requirement 29: 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. (GP-2)
- \_\_\_ Requirement 30: 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. (GP-2)
- \_\_\_ Requirement 31: 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. (GP-3)
- \_\_\_ Requirement 32: A breach of confidentiality must be immediately investigated to assess causes and implement remedies. (GP-4)
- \_\_\_ Requirement 33: 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. (GP-4)
- \_\_\_ Requirement 34: Laptops and other portable devices (e.g., personal digital assistants [PDAs], other handheld devices, and tablet personal computers [PCs]) 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. (GP-1)
- \_\_\_ Requirement 35: 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 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. Before any device containing sensitive data is taken out of the secured area, the data must be encrypted. Methods for sanitizing a storage device must ensure that the data cannot be retrievable using Undelete or other data retrieval software. Hard disks that contained identifying information must be sanitized or destroyed before computers are labeled as excess or surplus, reassigned to nonsurveillance staff, or before they are sent off-site for repair. (GP-1)

**Attachment B**



**DIVISION OF HEALTH  
AND MEDICAL SERVICES**

Community Health Services  
Disease Prevention  
Family Health  
Health Promotion  
State Epidemiologist

**Confidentiality Oath**

All Department of Health, Division of Health and Medical Services, 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. 25, issued: November 17, 2008, Title: HIPAA-General Provisions.

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 No. 31, issued: November 17, 2008, Title: HIPAA – General Provisions.
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, Division of Health and Medical Services, is the property of the Division of Health and Medical Services.
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 HIV Surveillance information with identifiers will also be supplied a copy of the Security Policy for HIV Surveillance and will follow all stipulations of the policy.

\_\_\_\_\_  
Employee, Contractor, or Intern Signature

\_\_\_\_\_  
Date

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

\_\_\_\_\_  
Director, Division of Health and Medical Services and  
Overall Responsible Party (ORP)

\_\_\_\_\_  
Date

Reviewed February 23, 2011

## Attachment C



### DIVISION OF HEALTH AND MEDICAL SERVICES

Community Health Services  
Disease Prevention  
Family Health  
Health Promotion  
State Epidemiologist

#### 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.

- 34-22-12.2** 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.

**Administrative Policies and Procedure, Statement No. 25, issued: November 17, 2008,**  
**Title: HIPAA-General Provisions.** Please see <http://intranet.state.sd.us/doh.policymanual.pdf>.

**Attachment D**  
South Dakota Department of Health  
Administrative Policies and Procedures

**STATEMENT NO. 25**

**TITLE: HIPAA – General Provisions**

**ISSUES: November 17, 2008**

The purpose of this policy is to set for 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 (PHI).  
*Protected Health Information* Individually identifiable health information, including demographic information, such as age, address, and account numbers, and information that related 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 from signed by program participants shall be retained by the DOH according to state retention policies for a period of six years.

**C. Right of Access, Inspect and Copy PHI (45 CFR § 164.524)**

Upon receipt of a written request, the DOH will provide program participants with access to their PHI maintained by the DOH, as required by law, and will offer program participants a review process when certain requests are denied. When access is provided, program participants will be allowed to obtain a copy of the information requested. However, the DOH may charge program participants for the reasonable costs associated with providing such access in accordance with *Administrative Policy Statement No. 17*.

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

Upon receipt of a written request, the DOH will provide program participants with an accounting of the DOH's disclosure of their 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 program participants for the reasonable costs associated with providing such disclosure in accordance with *Administrative Policy Statement No. 17*. The DOH may suspend a program participant's right to an accounting of disclosures under limited circumstances, as authorized by law.

South Dakota Department of Health  
Issued: November 17, 2008

Administrative Policies and Procedures Statement No. 25

**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)**

Program participants (or personal representative) may ask that the DOH take reasonable steps to ensure that communications with program participants remain confidential. This can be achieved by contact through an alternate means or location (Le., 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. Program participants (or personal representative) who feel their 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. Program participants may also file complaints directly with the federal Office for Civil Rights by calling 866-627-7748 or visiting [www.hhs.gov/ocr/hipaa](http://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 de-identifying 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 participants 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. 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. De-identified 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 the Career Service Act and application state administrative rules.

**Attachment E**



**DIVISION OF HEALTH  
AND MEDICAL SERVICES**

Community Health Services  
Disease Prevention  
Family Health  
Health Promotion  
State Epidemiologist

**CERTIFICATION REGARDING COMPLIANCE WITH SECURITY STANDARDS FOR THE PROTECTION OF HIV/AIDS SURVEILLANCE INFORMATION & DATA**

The undersigned has been designated as the overall responsible party (ORP) by the applicant organization. This official accepts overall responsibility for implementing and enforcing the security standards and may be liable for breaches of confidentiality. The ORP should be a high-ranking public official, for example, the division director or department chief over HIV/AIDS surveillance. This official should have the authority to make decisions about surveillance operations that may affect programs outside the HIV/AIDS surveillance unit and should serve as one of the contacts to public health professionals and the HIV affected community on policies and practices associated with HIV/AIDS surveillance. By signing, the ORP certifies that the applicant will comply with the “Security Standards for the Protection of the HIV/AIDS Surveillance Information & Data” by: (a) Acknowledging that all “**Program Requirements**” included in the “Security Standards for the Protection of HIV/AIDS Surveillance Information & Data” have been implemented, unless otherwise justified in an attachment to this statement. (b) Applying the “**Program Requirements**” to all local/state./territorial staff and contractors funded through CDC to perform HIV/AIDS surveillance activities. (c) Applying the “**Program Requirements**” at all sites where the Evaluation HIV/AIDS Reporting System (eHARS), or other HIV/AIDS surveillance database, is maintained.

Name and address of organization  South Dakota Department of Health Division of Health and Medical Services 615 East 4 <sup>th</sup> Street Pierre, SD 57501	
Phone no. (with area code) 605 773-3737	Fax no. (with area code) 605 773-5942
Name of ORP (print) Colleen Winter	Title Division Director Health and Medical Services
Signature	Date

### Attachment F

Table 1 Data System Access Role	Individual	Reporting Website	Maven	COHORT	eHARS	ACCESS LEVEL
Administrative Assistant						LL
Administrative Assistant						LL
Administrative Assistant						LL
Administrative Assistant						LL
Administrative Assistant						LL
Administrative Assistant						LL
Administrative Assistant						LL
Administrative Assistant						LL
Administrative Assistant Sioux Falls						LL
Administrative Assistant						LL
Administrative Assistant						LL
Summer Intern			X	X		
BIT Software Developer		X				A
BIT Web Administrator			X	X		A
BIT – DBA			X	X		A
BIT – DBA			X	X		A
BIT – DBA			X	X		A
BIT – DBA			X	X		A
BIT-DBA			X	X	A	
BIT - DBA			X	X		A
BIT Web Administrator			X	X		A
BIT Web Administrator			X	X		A
Super Users – Disease Surveillance Coordinator		X	X	X		A
Super Users – Disease Surveillance Manager		X	X	X		A
Super Users – Bioterrorism Surveillance Coordinator		X	X	X		A
Super Users – Bioterrorism Surveillance Coordinator		X	X	X		A
Super Users – Field Staff Coordinator		X	X	X		A
Super Users – Data Manager/GIS Mapping		X	X	X		A
Super Users – Data Manager/GIS Mapping		X	X	X		A
General Epi Program Manager – State Epidemiologist			X	X		X
General Epi Program Manager – Office Administrator			X	X		X
General Epi			X	X		X
HIV Surveillance Coordinator			X	X	X	X
STD Program Manager			X	X	X	X
TB Program Manager			X	X		X
Immunization Program Manager			X			X
Primary Investigator		X	X	X		X
Primary Investigator		X	X	X		X
Primary Investigator		X	X	X		X
Primary Investigator		X	X	X		X



## Attachment 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:** Advances 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).