SOUTH DAKOTA DEPARTMENT OF HEALTH

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)