ARKANSAS INFECTIOUS DISEASE BRANCH

Security and Confidentiality Policy, Protocols and Pledge

Purpose

This manual has been established to ensure the security and confidentiality of all data collected and/or disseminated by the Infectious Disease Branch of the Arkansas Department of Health. It specifies the terms of use and data sharing protocols to ensure the security and confidentiality of personal identifiable information collected by Programs within the Branch as a result of infectious disease reporting. Arkansas State law requires that all cases of Sexually Transmitted Infections, HIV, Hepatitis C and Tuberculosis be reported to the Department by physicians, hospitals, infection control practitioners and/or chairpersons of hospital infection control communities, directors of all laboratories doing business in the State of Arkansas, medical directors of in-home health agencies, program directors of all state agencies, nursing home medical directors and other persons as required by the rules and regulations of the Arkansas Department of Health.

Assurance

The Infectious Disease Branch of the Arkansas Department of Health respects and appreciates the public and provider concerns regarding security and confidentiality of Personal Identifiable Information (PII). The Branch upholds the foremost regard for the public confidence in its ability to maintain all PII in the strictest of confidence and security.

Guiding Principles

1. Public health data should be acquired, used, disclosed and stored for legitimate public health purposes.
2. Programs should collect the minimum amount of personally identifiable information necessary to conduct public health activities.
3. Programs should have strong policies to protect the privacy and security of personally identifiable data.
4. Data collection and use policies should reflect respect for the rights of individual and community groups and minimize undue burden.
5. Programs should have policies and procedures to ensure the quality of any data they collect or use.
6. Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.
7. Programs should share data for legitimate public health purposes and may establish data-use agreements to facilitate sharing data in a timely manner.
8. Public health data should be maintained in a secure environment and transmitted through secure methods.
9. Programs should minimize the number of persons and entities granted access to identifiable data.
10. Program officials should be active, responsible stewards of public health data.

Program Policies and Responsibilities

Standard 1.1 The Branch has the responsibility to develop a set of written policies and procedures on data security and confidentiality. These policies must be reviewed and updated on an annual basis ensuring that all staff having access to personal identifiable information are trained and annually attest to receipt and compliance with the policy.

Annually, the Surveillance Program Manager and the Branch Chief will assess the current policies pertaining to security and confidentiality of all data collected, maintained and disseminated by Programs within the Branch.

Standard 1.2 The Branch shall have a designated Overall Responsible Party (ORP) who shall ensure the security and confidentiality of public health data collected or maintained by programs within the Branch and ensure that the ORP is named in policy documents related to data security.

The ORP for data collected, maintained and disseminated by the Branch is Namvar Zohoori, Deputy Director for Science

Standard 1.3 The Branch shall ensure that data access levels and roles are defined clearly in the policy and all authorized access to confidential public health data containing personal identifiable information has clear procedures for accessing data securely.

Surveillance staff, authorized members of the field, Ryan White and HIV Prevention Program staff within the Infectious Disease Branch shall have access to data that are collected as a result of daily public health and surveillance activities. This includes paper copies of reports and databases containing personally identifying information.
Note: access to individual client level data and databases are designated on a need to know basis.

The Branch shall release information for statistical purposes in aggregate. Data requests for individual client level data will be reviewed by the appropriate legal authorities within the agency and handled on a case-by-case basis according to state and federal statutes. The Arkansas Infectious Disease Branch data release policy includes contingencies for releasing data with both small numerators and denominators. The Branch utilizes the national practices of non-release of cell sizes less than five (5) in efforts to ensure confidentiality of cases in areas having small population sizes. Cell sizes less than five (5) will not be displayed or released beyond state, regional (multicounty) or MSA (Metropolitan Statistical Area) <500,000 level. In efforts to preserve confidentiality of individuals in less densely populated areas of the state, requests for cross tabulation of data at the county level will be governed by the Program's data release policy.

Standard 1.4 The Branch will ensure that data security polices require ongoing reviews of evolving technologies and includes a computer back-up or disaster recovery plan.

An annual assessment of the computer networks, servers and databases shall be conducted to ensure that there are adequate and sufficient security protocols and processes in place to ensure the safety and integrity of all electronic data collected and maintained by the section within its databases. There will also be regular assessments of backup servers, facilities and practices to ensure nightly data backups and the ability to have emergency retrieval of Program data if and when necessary.

An evaluation of new technologies, software and network servers shall be required prior to being applied to surveillance databases, program activities, etc.

Standard 1.5 The Branch will ensure that any breach of data security protocol regardless of whether personal information was released, is reported to the ORP and investigated immediately. Any breach that results in the release of PII to unauthorized persons should be reported to the ORP, to the Centers for Disease Control and Prevention (CDC), and, if warranted, to law enforcement agencies in accordance with state and federal law.

All instances of either breach of protocol or breach of policy shall be documented, fully investigated and reported to the Surveillance Programs Manager, Branch Chief and the ORP. In the event that the breach involves the release of PII to unauthorized persons, the incident shall also be reported to the Office of the General Counsel, the Director of Health, the CDC and, if warranted, to law enforcement agencies in accordance with state and federal law.

Standard 1.6 The Branch will ensure that staff members with access to identifiable public health data attend data security and confidentiality training annually.

Every staff member (including students, volunteers and contractors) of the Branch is required to participate in the annual security and confidentiality training. In addition to Branch staff members, all Information Technology (IT) personnel having access to servers, workstations and databases for the Infectious Disease Branch shall participate in the annual training. The Branch Chief shall be responsible for ensuring that trainings occur and all required staff members are in attendance.

Standard 1.7 The Branch shall require all newly hired staff members to sign a confidentiality agreement before being given access to identifiable information and require all staff to re-sign their confidentiality agreements annually.

At the time of orientation to the Branch, new employees are required to review the policy and complete the Security and Confidentiality training and post test assessment.

All staff shall certify annually, compliance with training and attestation of understanding and receipt of policies regarding security and confidentiality of all data collected, maintained and disseminated by programs within the Infectious Disease Branch of the Arkansas Department of Health.

Standard 1.8 The Branch shall ensure that all persons having authorized access to confidential public health data take responsibility for 1) implementing the Program's data

security policies and procedures, 2) protecting the security of any device in their possession on which PII are stored, and 3) reporting suspected security breaches.

Everyone is responsible for ensuring the security and confidentiality of Surveillance data and Program information containing PII.

Standard 1.9 The Branch shall certify annually that all data security standards have been met.

Each Program shall complete the attestation form noting compliance with CDC grant deliverables for ensuring the security and confidentiality of all data collected, maintained and disseminated by Programs of the Infectious Disease Branch.

Standard 2.1 The Branch shall clearly specify the purpose for which the data will be collected.

All data collected, maintained and disseminated by Programs within the Branch are for the sole purpose of conducting public health activities; in addition to ensuring the health and safety of persons in the State of Arkansas.

Standard 2.2 The Branch shall collect and use the minimum information needed to conduct specified public health activities and achieve the stated public health purpose.

All data collected by Branch Programs shall be for the sole purpose of conducting public health activities such as surveillance monitoring, case investigation, prevention and intervention initiatives. The Programs shall collect, at a minimum, demographics and locating information pertaining to an individual person suspected of being infected to begin and carry out case investigation activities.

Standard 2.3 The Branch shall collect personally identifiable data only when necessary; use no identifiable data whenever possible.

All data collected by Programs of the Branch require identifiable elements and are to be maintained in the most secure of environments and confidentiality ensured and protected. The Branch shall ensure that all data released and/or disseminated is done in de-identified aggregate format to ensure the confidentiality of the individual and small populations.

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

Access to any case specific surveillance information beyond routine surveillance activities shall require a formal data request delineating specifics of desired data, approval by the Surveillance Programs Manager, ORP and the agency SAC (Scientific Advisory Committee)

approval. All research related requests shall be directed to the ORP for review and referral for SAC approval.

Standard 3.1 The Branch will limit the sharing of confidential or identifiable information to those with a justifiable public health need; ensure that any data sharing restrictions do not compromise or impede public health programs or disease surveillance activities and that the ORP or other appropriate official has approved this access.

To ensure timely intervention and prevention of further spread of communicable diseases within the population, the Infectious Disease Branch Surveillance Programs will share limited identifiable information on a need to know basis to ensure public health action occurs in a timely manner. Data will be shared upon request to authorized public health partners ensuring the ability to maintain the security and confidentiality of the privileged information.

Standard 3.2 The Branch shall assess the risks and benefits of sharing identifiable data for other than their originally stated purpose or for purposes not covered by existing policies.

All special data requests for individual person level data shall be assessed and approved by the Surveillance Programs Manager and then moved on to the Branch Chief and the ORP for final approval and if necessary to the agency legal counsel for review.

Standard 3.3 The Branch shall ensure that any public health program with which personally identifiable public health data are shared has data security standards equivalent to those in this document.

Any and all requestors of individual client level data must be able to ensure and prove compliance with the standards and policy guidelines outlined herein for the Branch prior to consideration of data sharing.

Standard 3.4 The Branch shall ensure that public health information is released only for purposes related to public health, except where required by law.

Any and all requests for individual client level identifying information requested by other entities (law enforcement, court representatives, etc.) outside of the realm of public health shall be referred to Arkansas Department of Health Office of General Counsel for review and approval.

The Surveillance Coordinator will defer to the ORP and Arkansas Department of Health Office of General Counsel on any requests for identifiable information not used for public health purposes.

Any release of client specific information must be reviewed and authorized by the following personnel: The Surveillance Programs Manager, the Infectious Disease Branch Chief, the ORP (the Deputy Director for Science) and the Office of General Counsel.

Standard 3.5 The Branch shall establish procedures, including assessment of risks and benefits for determining whether to grant a request for aggregate data not covered by existing data-release policies.

Data requests beyond the normal nature of requests shall be reviewed by both the Surveillance Programs Manger and the Branch Chief for approval to fill the request.

In some instances, access to surveillance data or information without identifiers may still require ORP approval. Approval of a release of information by the Branch Chief will only be given after a justification of the need has been determined.

Standard 3.6 The Branch shall disseminate non-identifiable summary data to stakeholders as soon as possible after data are collected.

The Surveillance Program will disseminate annual reports and epidemiologic profile data to key stakeholders on a regular basis. All data presented will be in aggregate form and displayed in a manner that protects the confidentiality of individuals. Cell sizes less than five (5) will not be displayed or released beyond state, regional (multicounty) or MSA (Metropolitan Statistical Area) <500,000 level. In efforts to preserve confidentiality of individuals in less densely populated areas of the state, requests for cross tabulation of data at the county level will be governed by the Program's data release policy.

Standard 3.7 The Surveillance Program shall assess data quality before disseminating data.

All data collected shall be regularly evaluated, cleaned and analyzed for accuracy and validity prior to release for public consumption.

Standard 3.8 The Surveillance Programs Manager shall ensure that data-release policies define purposes for which the data can be used and provisions to prevent public access to raw data or data tables that could contain indirectly identifying information.

All requests for data must be submitted to the Infectious Disease Branch Surveillance Program via the Surveillance Program data request form. A description of the data requested along with the intended purpose and need for the data must be specified in detail on the request. All details regarding security, maintenance, presentation, dissemination and intended audience of the data must be specified.

Any and all data released will follow the guidelines for suppression as outlined within this document.

Standard 4.1 The Branch shall, to the extent possible, ensure that persons working with paper copies of documents containing confidential, identifiable information do so in a secure locked area.

All staff having access to Surveillance Program data or data containing PII shall work inside of secure offices having working locks on doors and windows. The offices shall have limited

access to the public. All suites within the Infectious Disease Branch shall have keycard access for authorized personnel only. All offices will have individually keyed locks. All hard copy files and documents shall be contained in file cabinets having working locks and limited keycard access.

Standard 4.2 The Branch shall ensure that documents containing confidential information are shredded with crosscutting shredders before disposal.

All documents must be shredded prior to disposal to ensure destruction of identifiers. All Branch Programs will have access to commercial grade shredders having crosscutting or confetti cut features to ensure proper destruction of documents.

All documents shall have personal identifiers removed prior to disposal. All documents must be shredded using crosscutting shredders prior to disposal.

Programs may use shredding lock boxes provided by contracted vendors that conduct mass shredding of confidential and protected health information.

Standard 4.3 Each Branch Program shall ensure that data security policies and procedures address handling of paper copies, incoming and outgoing mail, long-term paper storage, and data retention guidelines. The amount of confidential information in all such correspondence should be kept to a minimum and destroyed when no longer needed.

All paper copy documents maintained by Programs of the Branch including documents containing PII shall be stored in locked file cabinets within locked offices maintained within secure suites having keycard access for authorized personnel.

According to agency record retention regulations Section 1.18.665, Arkansas Administrative Code, the Branch will maintain paper copy files of individual cases for a minimum of ten (10) years.

All staff having access to information with PII shall annually attest to attending and complying with the policies outlined in the security and confidentiality training.

While conducting routine work in the field or offices, staff will work to maintain the security and confidentiality of all documents. Confidential information shall not be left in public access areas. All data taken from or transported to offices over the course of the workday shall contain as little PII as possible and shall be maintained in secure locked brief cases.

Incoming and Outgoing Mail

All incoming and outgoing mail shall be processed in the following manner: All packaging shall be addressed to a specific individual, marked ‘confidential’ and shall not make any reference to any disease or condition anywhere on the packaging.

All incoming and outgoing mail containing PII shall be double sealed and double enveloped with the inside envelope sealed, stamped 'confidential', and addressed to a specific individual.

Mail Distribution
All incoming mail is opened, sorted date stamped and distributed among Surveillance Program staff on a daily basis. Once the mail is processed and entered, it is stored and secured in a locked room in locked filing cabinets each night.

Standard 4.4 The Branch shall limit access to secure areas that contain confidential public health data to authorized persons only and establish procedures to control access to secure areas by non-authorized persons.

Only authorized personnel are allowed in the secure Branch suites. Both suites of the Branch have keycard only access. The Branch Chief maintains the list of all personnel authorized to access the suites. Any visitors must be escorted through the suite by authorized personnel at all times. Visitors are not authorized to access private office areas without authorized personnel escorts.

Standard 4.5 The Branch shall ensure that Program personnel working with documents containing PII in the field 1) return the documents to a secure office area by close of business, 2) obtain prior approval from the program manager for not doing so, or 3) follow approved procedures for handling such documents.

While conducting routine field activities, staff shall ensure that documents contain limited PII. All such documents shall be contained in secure locked brief cases and maintained in locked automobiles until transported back to the office. Prior approval must be granted by the Surveillance Programs Manager to maintain documents outside of the office overnight.

Standard 4.6 The Branch shall ensure that documents with line lists or supporting notes contain the minimum amount of potentially identifiable information necessary and if possible, that any potentially identifiable data are coded to prevent inadvertent release of PII.

All documents taken into the field shall have limited PII. Staff will utilize appropriate codes in efforts to minimize the amount of PII on documents used in the field.

Standard 5.1 The Branch shall ensure that analysis datasets that can be accessed from outside the secure area are stored with protective software (i.e., software that controls data storage, removal and use) and verify removal of all personal identifiers.

Any and all datasets containing PII shall be encrypted and stored on secured networks having limited access to authorized personnel only. All computers shall be password protected and utilize screensavers to minimize unauthorized access.

Standard 5.2 The Branch shall ensure that any electronic transfer of data is approved by the ORP and subject to access controls and that identifiable data are encrypted before being transferred.

Requests for any and all data containing PII shall be formally requested utilizing the Branch's official data request form and reviewed by the Surveillance Programs Manager and shall have the approval of the Branch Chief and ORP. Any and all electronic data transfers shall be encrypted and secured prior to transfer.

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

Surveillance activities involving PII are usually conducted only in the Surveillance Program secured area. Storage media include floppy disks, CD's, and encrypted USB keys; those used for confidential information shall be discretely labeled and all data secured by encryption.

When data are moved between workstations using storage media, the storage media must remain in the secured area, be accounted for at the end of the workday and then be stored and secured in a locked cabinet.

Only minimum identifiable information needed for a given task shall be placed on storage media. Entire databases are not to be moved without sound justification and prior approval from the Branch Chief.

Identifiable information on storage media shall be deleted from the device and the device erased and sanitized to ensure that data are rendered completely unreadable. If the media will no longer be used, efforts should also be made to physically damage the media prior to disposal.

Emailing of unencrypted PII is not allowed in efforts to prevent unintended release of confidential information.

Standard 5.4 The Branch shall use encryption software that meets federal AES standards to encrypt data with PII on all laptops and other portable devices that receive or store public health data with personal identifiers.

Any laptops or portable devices that receive and/or store public health data containing PII shall require password protection and all dataset must be password protected and/or encrypted. All portable computer equipment and devices must be secured when not in use. Portable devices without removable or external storage components must have encryption software that meets federal AES standards.

All removable or external storage devices containing PII must be sanitized immediately following final use. Methods used to sanitize/erase storage devices must ensure that any data on the device cannot be retrieved by using "undelete" or data retrieval software. Hard drives, flash drives, copiers, printers, fax machines, and any other storage media of computers or other equipment having internal storage devices that once contained PII must be erased and/or physically destroyed before being labeled as excess or surplus, reassigned or sent off-site for repair.

Standard 5.5 The Branch shall ensure that data policies include procedures for handling incoming and outgoing facsimile transmissions. Minimize inclusion of PII in fax transmissions, and destroy paper copies and sanitize hard drives when no longer needed.

Use of facsimile to transmit and receive information pertaining to HIV, STI, Viral Hepatitis and Tuberculosis is allowed; however, extreme caution should be used to limit the inclusion of PII in the fax transmission. Fax usage should be conducted in the secure restricted access area. The Surveillance Programs currently use a secure desktop fax housed on a separate secure network with access granted only to Surveillance Program staff. Each staff member has their own secure folder on the network where incoming faxes are received. Each staff member's fax folder is secured with their network login password. There is also an exclusive secured physical fax machine located in the HIV Surveillance records room accessed only by HIV Surveillance staff for confidential lab and case reports being sent and received by the HIV Surveillance Program.

Documents containing PII being sent from programs within the Branch that may present a potential confidentiality risk should be transmitted using a generic fax cover sheet and only the minimum amount of identifiers necessary. When sending faxes, program staff will ensure that the recipient of the documents have been contacted and are awaiting the transmittal of the documents and confirm receipt of sent information. All staff utilizing facsimile as a transmission method should take extra precaution to verify the phone number of the intended recipient prior to sending documents.

When fax machines are retired, the memory storage and hard drives should be sanitized and destroyed before disposal and removal from the program.