ARIES Security Policy

Policy Number  231.001
Effective Date  August 18, 2010
Revision Date  December 23, 2019
Subject Matter Expert  Services Data Internal Workgroup
Approval Authority  HIV Care Services Group Manager

1.0 Purpose
This policy defines security standards for protecting the confidential information collected and maintained in the AIDS Regional Evaluation System (ARIES) database by the HIV Care Services Data Group within the HIV/STD program. This policy addresses the administrative, physical, and technical safeguards for the security of ARIES and confidentiality of client information.

This policy describes the actions required of the Texas Department of State Health Services (DSHS) HIV/STD Program, Administrative Agencies (AA), and HIV service provider agencies that handle confidential client information collected and reported through ARIES. This policy also outlines procedures for data managers and HIV service provider registration authorities to use when authorizing and assigning roles, rights, and permissions to users as well as when securing data and systems, both physically and electronically.

2.0 Background
In fulfilling its mission to facilitate and assess need for HIV services, the DSHS HIV/STD program, its contractors, and external partners obtain confidential information about individuals they serve. These individuals trust that the HIV/STD program will take every precaution to protect that information to ensure their confidentiality. The HIV/STD program and Administrative Agency must be vigilant in maintaining the integrity of the system (ARIES) that stores this confidential information.

3.0 Authority
Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C; Texas Government Code 2054, Information Resources Management Act

4.0 Definitions
Administrative Agency (AA) - Entity under contractual agreement with the Department of State Health Services to manage and distribute federal and state funds to HIV Service Provider(s).

Administrative Agent – An individual within an Administrative Agency who is responsible for fulfilling contractual agreements as determined by the Department of State Health Services.

AIDS Regional Information and Evaluation System (ARIES) - Web-based, client-level software that Ryan White and State Services HIV Providers use to report all Ryan White and State Services provided to Ryan White eligible clients.

ARIES Authorized User - Individuals employed by an Administrative Agency or HIV service provider, who have been granted access to confidential information in order to carry out their assigned duties.

Advanced Encryption Standard - The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data.

Confidential Information - Any information about a patient that is intended to be kept in confidence or secret, and if released could result in the identification of the patient.

Confidentiality - The ethical principle or legal right patients and research participants have that ensures their confidential information is protected from unauthorized disclosure by physicians, other health professionals, or researchers with whom they share this information.

Data Managers - Staff at the Administrative Agency responsible for providing support to local organizations that utilize ARIES to report their HIV related service delivery.
Encryption - The manipulation or encoding of information so that only parties intended to view the information can do so. There are many ways to encrypt information; most commonly available systems involve public key and symmetric key cryptography.

Fifty Rule – This refers to the acceptable threshold for the release of aggregate HIV/AIDS and STD surveillance, epidemiologic, and public health follow-up data. The underlying population of the statistic released must be a population of greater than fifty people. The underlying population must also be at least twice the number of cases.

Local Responsible Party (LRP) - An employee of an Administrative Agency, such as an Administrative Agent, who accepts responsibility for overseeing the implementation, enforcement, and maintenance of ARIES security and confidentiality policies and procedures at their own agency, as well as at all entities with whom they have contractual relations (e.g. contracted providers, sub-contracted providers, etc.). The LRP is also responsible for reporting and assisting in the investigative privacy incident process. The DSHS HIV/STD Prevention and Care Branch Manager is designated as the LRP for all DSHS staff and grantees working with the Minority AIDS Initiative (MAI).

Negligence - Negligence is the failure to use reasonable care. It is the failure to do (or not to do) something that a reasonably prudent person would do (or not do) under like circumstances. A departure from what an ordinary reasonable member of the community would do in the same community. Negligence is a 'legal cause' of damage if it directly, and in natural and continuous sequence, produces or contributes substantially to loss, injury, or damage, so it can reasonably be said that if not for the negligence, the loss, injury, or damage would not have occurred.

Password Protected - When files and directories are password protected from unauthorized access, a user name and password must be entered before access to protected files and directories is allowed.

Personal Identifier - A datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty; a personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

Privacy Incident - An incident in which confidential information, such as protected health information, might have been divulged to unauthorized parties and/or protocol for handling of confidential information might not have been followed.

Protected Health Information (PHI) - Any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

Registration Authorities (RA) - An employee of a service provider agency recognized by the LRP whose identity has been verified by an Administrative Agency data manager or DSHS Central Office staff who is responsible for verifying the identity and 'need-to-know' requirement for a new Authorized User request. Registration authorities are responsible for initiating new account requests and training as well as changes to existing accounts, including account termination.

Removable Storage Device - A device that allows for the transportation of electronic information; there are many types including, but not limited to: USB port flash drives (memory sticks), diskettes, CD-ROMS, zip disks, tapes, smart cards, and removable hard drives.

Secured Area - A confined physical space within the Administrative Agency or HIV service provider agency where patient information and ARIES data is located and entry is limited to staff with authorized access.

Secured Socket Layers - A cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message and allows
a secure connection between a client and a server, over which any amount of data can be sent securely.

Security - The protection of data and information systems, for the purposes of (1) preventing unauthorized release of identifying surveillance information or data from the systems (e.g., preventing a privacy incident) and (2) protecting the integrity of the data by preventing accidental data loss or damage to the systems. Security includes measures to detect, document, and counter threats to the confidentiality or integrity of the systems.

Service Provider Agency - Organization(s) under contractual agreement with Administrative Agency to provide HIV-related medical and psychosocial support services to person(s) living with HIV/AIDS. HIV service provider agencies are required to enter relevant data into ARIES per their contractual agreement with the Administrative Agency.

Violation of Confidentiality - A finding by the DSHS Privacy Office that established state and/or federal protocols governing the secure handling of confidential information were not followed and that confidential information was divulged to unauthorized parties.

Violation of Protocol - A finding by the DSHS Privacy Office that established state and/or federal protocols governing the secure handling of confidential information were not followed.

Wi-Fi (Wireless Fidelity) - Refers to wireless network components that are based on one of the Wi-Fi Alliance’s 802.11 standards. The Wi-Fi Alliance created the 802.11 standard so that manufacturers can make wireless products that work with other manufacturers’ equipment. This equipment uses high-frequency radio waves rather than wires to communicate. Wi-Fi is commonly used to wirelessly access the Internet or a local network.

5.0 Policy
It is the policy of DSHS HIV Care Services that ARIES and the information collected and stored in ARIES are protected and maintained to ensure patient confidentiality.

6.0 Persons Affected/Applicability
This policy applies to Local Responsible Party, Administrative Agency, Administrative Agency data managers, registration authority, Department of State Health Services, and all other ARIES authorized users who could potentially view and/or have access to ARIES and confidential information entered and stored in the database.

7.0 Responsibilities

7.1 Department of State Health Services
The Department of State Health Services (DSHS) is responsible for enabling and terminating ARIES user account access at the request of the Administrative Agency data manager, or at DSHS’ discretion. DSHS is also responsible for handling security incidents and breaches and must be notified by the LRP, AA, data manager or local HIV provider of any security incidents or breaches.

7.2 Administrative Agency (Agent)
As the entity that manages HIV service provider contracts and with whom the Local Responsible Party (LRP) is employed, the Administrative Agency is responsible for executing and overseeing all security and confidentiality requirements as outlined in this policy. The Administrative Agency or Agent will be required to designate an LRP and data manager within their own agency, as well as a registration authority at each subcontracted HIV service provider. Any changes to the aforementioned roles must be reported to DSHS within five (5) business days.

The Administrative Agent and/or LRP must assign one or more employees from their Administrative Agency to fulfill the following duties:
- Maintain a list of active ARIES users and notify DSHS whenever there are any changes;
- Ensure all authorized users submit a signed confidentiality form annually;
- Monitor user rights on a quarterly basis or when an employee changes position or terminates and notify DSHS to make appropriate changes as needed;
• Train authorized users how to use ARIES and ensure authorized users understand all security and confidentiality requirements;
• Ensure all authorized users complete an annual security training.

The following security and confidentiality information must be communicated to all ARIES users: ARIES users are individually responsible for ensuring that the confidential information they work with is protected. This responsibility includes protecting all passwords, keys, and codes that enable access to confidential information;
• ARIES users are responsible for reporting possible security risks to the LRP;
• ARIES users are individually responsible for protection of his/her own desk/work area, workstation, laptops or other devices associated with confidential information;
• ARIES passwords may not be shared with anyone and no one should access ARIES using another person’s login credentials (not even other users)
• ARIES users are responsible for challenging and reporting those persons who are not authorized to access confidential information;
• Confidential information gained in the course of work activity will not be divulged to unauthorized persons; and
• Upon resignation or termination, all confidential information and keys or devices that enable access to physical and electronic locations where confidential information may be stored must be returned to his/her immediate supervisor.

7.3 Local Responsible Party
The Local Responsible Party (LRP) is responsible for implementing and enforcing security and confidentiality policies and procedures. Duties the LRP must fulfill include:
• Investigating suspected privacy incidents and reporting these incidents to DSHS when necessary.
• Approving ARIES account requests that are submitted by the registration authority at individual HIV service providers. The LRP is the required signature authority for all ARIES authorized users as subcontracted by the Administrative Agency.
• Ensuring confidential information housed in the ARIES data system is accessed only by individuals who have signed and submitted all necessary documentation for ARIES access and have a “need-to-know” role in their respective position within an HIV service provider agency, DSHS, or Administrative Agency.

7.4 Data Managers
Administrative Agency data managers must ensure all users are authorized and that each authorized user has the correct permissions within the system. For example, users who do not need to see medical or risk information should not be given rights to those screens. The data manager must limit access to ARIES data through assignment of user permissions appropriate for a user’s role. Only DSHS and Administrative Agency data managers have rights to ARIES Report/Export. The Administrative Agency data managers must not grant ARIES Report/Export rights to any other users.

The data manager is responsible for ensuring authorized users have completed and signed security certificate documentation and that the LRP has signed the user request form prior to requesting ARIES account creation from HHSC/DSHS IT.

7.5 Registration Authority
The registration authority at a local HIV service provider is responsible for identifying appropriate authorized users and requesting ARIES access on the employees’ behalf, only after all required documentation has been signed by the employee, using the Department of State Health Services’ Account Request form. The registration authority must coordinate with their data manager to complete a deactivation form to terminate an authorized user account and must notify their data manager within 24 hours of any changes to account permissions within ARIES.

The registration authority will coordinate with the Administrative Agency data manager to verify the identity of all authorized users, ensure that authorized users complete and sign a confidentiality
agreement, acceptable use agreement and complete necessary security and HIPAA training per the guidelines set forth by local HIV service provider, Administrative Agency and Department of State Health Services.

7.6 Authorized User
Authorized users are responsible for completing the confidentiality agreement, acceptable use agreement and necessary security and HIPAA training per the guidelines set forth by local HIV service provider, Administrative Agency and Department of State Health Services. ARIES users are individually responsible for ensuring that the confidential information they work with is protected. This responsibility includes protecting all passwords, keys, and codes that enable access to confidential information;

- ARIES users are responsible for reporting possible security risks to the LRP;
- ARIES users are individually responsible for protection of his/her own desk/work area, workstation, laptops or other devices associated with confidential information;
- ARIES users are responsible for challenging and reporting those persons who are not authorized to access confidential information;
- Confidential information gained in the course of work activity will not be divulged to unauthorized persons; and
- Upon resignation or termination, all confidential information and keys or devices that enable access to physical and electronic locations where confidential information may be stored must be returned to his/her immediate supervisor.

8.0 Procedures

8.1 Procedures for submitting ARIES account requests

- Registration Authority: The RA at local service provider sites will identify staff who require access to ARIES and will complete the RA section of the account request form. The RA will send the account request form, proof of security or HIPAA training, confidentiality agreement, and acceptable use agreement to their data manager to begin the account provisioning process.
  - Authorized User: Each authorized user must submit an Account Request form, as well as provide documentation of completed security and HIPAA training, a completed and signed DSHS confidentiality agreement and acceptable use agreement. Proof of security training and a signed confidentiality agreement must be renewed by each user on an annual basis.

- Data Manager: The data manager for each Administrative Agency will receive account request forms from the local service provider sites. Once received, the DM will review the form and assign the new user a role in ARIES in the Data Manager section of the form. The DM will send the account request form and other required documents to the LRP for final approval. Once the signed and completed account request form is received back, the DM will work with the new user to create an ARIES profile and request approval for an ARIES certificate from HHSC/DSHS IT for the new user’s computer. When ARIES certificate is approved by DSHS, DM will work with new user to get ARIES activated on the user’s computer. DM will keep track of the user’s permissions in the account request form.

The data manager is the individual responsible for submitting ARIES account requests to HHSC/DSHS IT for all users under their purview.

- LRP: The LRP will sign the account request form only after all new user required documentation has completed and submitted by the data manager. Once signed, the LRP will return the account request form to the data manager for ARIES account creation.

- HHSC/DSHS IT: HHSC/DSHS IT will fully provision ARIES account for authorized users after notification has been received from the LRP or data manager.
Figure 1 ARIES New User Account Request Procedure

* Supporting documentation includes: confidentiality agreement, acceptable use agreement and security and/or HIPAA training certificate

8.2 Procedures for revoking ARIES account access
- Registration Authority: The RA at local service provider sites will identify staff who no longer require ARIES account access, or whose permissions need to be altered due to changes in job
requirements or employment status. RA will notify their data manager to begin the process to revoke or change account permissions.

- **Data Manager:** The data manager will fill out the DSHS account deactivation form and contact HHSC/DSHS IT within 24 hours to terminate or change ARIES account permissions for specified account holders.

- **HHSC/DSHS IT:** HHSC/DSHS IT will terminate or change ARIES account permissions within 24 hours of data manager requests.

### 8.3 Procedures for managing ARIES Users

- The Administrative Agency is responsible for maintaining the ARIES user log and will send the log to the DSHS/TB/HIV Section Security Officer at the end of every quarter.

### 8.4 Procedures for ARIES Data Requests

Releases of electronic client level data files to third parties for grant development, research, needs assessment, creation of reports or any other purpose must not be made without DSHS approval, and DSHS reserves the right to require the party requesting the data submit the request to DSHS’ Institutional Review Board if the request appears to be related to research or includes a request for the release of client identifying information.

Routine requests for utilization reports and aggregate profiles of clients served from staff other than funded providers or Administrative Agency staff may be released without consultation with DSHS, but must comply with the [Release of TB/HIV/AIDS and STD Data Policy 302.001](#). Aggregate profiles of client characteristics that include cross-tabulated tables with cells that do not meet the Rule of Fifty should be released only after such cells have been redacted and replaced with a mark indicating a small cell count precludes inclusion of the specific figure. Requests can be submitted to ARIESData@dshs.texas.gov

### 9.0 Physical Security

#### 9.1 Secured Areas

All confidential information must be maintained in a secure area. A secure area is an area that is protected by at least two levels of physical security. Examples of physical security include a secured access card reader, locked door, locked immobile cabinets. Visitors that enter a secured area where confidential information is stored must be signed in and out and escorted by an authorized staff member at all times.

The physical security of the building containing the confidential information must be approved by both the provider RA and the Administrative Agency data manager.

#### 9.2 Computer Workstations

All computer workstations with access to ARIES data must be physically located in a secure area. Workstations with access to ARIES must be password protected at the Windows login level and have a password protected screensaver program enabled. The screensaver should be set to automatically activate in 5 minutes or less when the workstation is not in active use.

- Computer passwords are unique to the authorized user and must not be shared with others.
- If a password’s security is in doubt, it must be changed immediately.
- Authorized users are responsible for locking computer workstations (Ctrl/Alt/Delete - Lock Workstation) when a workstation is left unattended.
- Computer screens must not be readily observable by non-authorized users as they pass through the office area or approach reception desk. Security screens may be installed on computer monitors to prevent viewing of information on the computer screen by anyone other than authorized user.
ARIES must not be accessed from unsecured or public networks, networks not administered by an Administrative Agency or HIV service provider agency, or networks that do not meet the requirements of this policy.

10.0 Laptops and Portable Devices
All staff authorized to access ARIES are individually responsible for protecting assigned mobile devices used to access ARIES or store confidential information which originated from ARIES.

10.1 Laptops
Laptops used as a work computer fall under the same confidentiality and security guidelines as indicated under section 9.2 Computer Workstations. ARIES security certificates will be installed on laptop computers only with DSHS approval and under the following requirements:
- There is a signed ARIES Laptop Agreement that can be obtained from Administrative Agency;
- DSHS approves the signed agreement;
- The laptop user has a separate signed statement indicating receipt and understanding of laptop agreement/requirements;
- Laptop hard drives must be encrypted using encryption software meeting Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and password protected. Passwords must be stored separately from the device.

10.2 Remote Laptop Security
Staff traveling to or from a site visit with an HIV service provider, Administrative Agency, or DSHS must secure their individual work issued laptop using the following protocol:
- Laptops must be password protected and locked while traveling and not in use;
- Laptops must remain in physical contact with the authorized laptop user at all times while offsite. When traveling by car is necessary, the laptop must be locked in the trunk of the authorized laptop user’s car or remain on the physical person;
- Laptops must not be used for ARIES access in areas that are not physically secured by at least two levels of protection;
- Laptops must not be used for ARIES access on unsecure networks or networks that are not managed by entities listed in this policy.

10.3 Removable Storage Devices
All confidential information placed on a removable storage device must be encrypted using encryption software meeting Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and they should be password protected.
- When taking confidential data stored on removable storage devices from one secure area to another secure area, data must be encrypted, minimized to the essential data required, and stored on devices that are kept secure.
- Any removable storage device containing confidential information is to be stored following the physical and electronic standards of this document.
- Removable storage devices containing confidential information must not be taken to a private residence unless specific permission has been granted by DSHS.
- Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse. Alternatively, the diskettes and other storage devices may be physically destroyed (e.g., by incineration, shredding). Such physical destruction would include the device, not just the plastic case around the device.

10.4 Other Mobile Devices
Mobile devices other than laptops with encrypted hard drives will not be used to access, store or transmit confidential information which originated from ARIES.

11.0 Handling Electronic Data
11.1 Electronic Data Access
Access to ARIES will only be granted as defined in the ARIES User Policy (231.000).
• ARIES may be accessed solely by the person whose name is on the ARIES certificate used. Logins and certificates will be approved only for individual users; no generic or shared logins will be approved.
• Certificates will not be installed on roaming Windows profiles.
• Network drives containing confidential information must have controls in place that enable access to only authorized users.
• Staff may not attempt to access any data, program, or system for which they do not have approved authorization.

11.2 Electronic Data Transmission
• Only DSHS and Administrative Agency data managers have rights to ARIES Report/Export. Administrative Agency data managers must not grant ARIES Report/Export rights to any other users.
• Administrative Agency data managers must ensure that confidential data exported for the purpose of evaluation, monitoring, or quality assurance by the submitting agency or the Administrative Agency are physically and electronically secure and disposed of properly.
• Exported confidential information for the purpose of evaluation, monitoring, or quality assurance with the Administrative Agency or the submitting agency must not be taken to a private residence unless specific permission has been granted by DSHS.
• Use of a work computer from home in order to access ARIES is prohibited, unless expressly authorized by DSHS.

12.0 Evolving Technology
If the security guidelines specified in this policy do not cover evolving technology, it is the responsibility of the Administrative Agency data managers or HIV service provider registration authority to seek guidance of DSHS.

13.0 Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/13/2019</td>
<td>Updated policy to reflect changes in technology</td>
<td>All</td>
</tr>
<tr>
<td>9/26/2014</td>
<td>Converted format (Word to HTML)</td>
<td>-</td>
</tr>
<tr>
<td>8/18/2010</td>
<td>This is a new policy</td>
<td>-</td>
</tr>
</tbody>
</table>