TEXAS Department of State Health Services	**Policy Number**	**231.001**
	Effective Date	**July 19, 2011**
	Revision Date	**August 18, 2010**
	Subject Matter	**Services Data Internal Workgroup**
	Approval Authority	**Bexar County Ryan White Administrative Agency**

ARIES Security Policy

1.0 Purpose

This policy defines security standards for protecting the confidential information collected and maintained in ARIES by the HIV/STD program associated with HIV Care Services Data Group. 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, and service provider agencies which handle confidential client information collected and reported through ARIES. This policy also outlines procedures for data managers to use when authorizing, assigning roles, rights, and permissions to users, securing data and systems physically, as well as 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 regarding individuals they serve. These individuals trust that the HIV/STD program will take every precaution to protect that information in order to ensure their confidentiality. The HIV/STD program and Administrative Agency must be vigilant in maintaining the integrity of the system (ARIES) that contain 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)

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.

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

Breach of Confidentiality
A breach of protocol that results in the improper disclosure of confidential information: 1) accidentally or purposefully released verbally, electronically, or by paper medium, to an entity or person that by law does not have a right or need to know, or 2) purposefully accessed either in person or electronically by an entity or person that by law does not have a right or need to know.

Breach of Protocol
A departure from the established policies and procedures that may result in the improper disclosure of confidential information; an infraction or violation of a standard or obligation; this includes any unauthorized use of data, including de-identified data.

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 which pertains to a patient that is intended to be kept in confidence or secret which 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 researcher with whom they have share this information.

Data Managers
Staff at the Administrative Agency responsible for providing support to local organizations using ARIES to report their service delivery activities.

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.

Local Responsible Party (LRP)
An individual who accepts responsibility for implementing and enforcing ARIES security and confidentiality policies and procedures and has the responsibility of reporting and assisting in the investigative breach process.

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 personal identifier and password must be entered by requiring users before access 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.

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.

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 AA or service provider agency where ARIES data and information are located with entry 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 surveillance 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 breach of confidentiality) 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 AA to provide HIV-related medical and psychosocial support services to person(s) living with HIV/AIDS. Service Provider Agencies are required to enter relevant data into ARIES per their contractual agreement with the AA.

Suspected Breach
An alleged infraction or violation of a standard that may result in unauthorized disclosure of confidential information.

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 collect in ARIES is protected and maintained to ensure patient confidentiality.

6.0 Persons Affected/Applicability

This policy applies to all Administrative Agency data managers and other ARIES authorized users who could potentially view and/or have access to ARIES and confidential information.

7.0 Responsibilities

The AA Data Managers and Agency Management must certify all users attend ARIES training before granting access to the System. The AA data managers must also 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. In addition, AA data manager must maintain a list of ARIES users, monitor user rights on a quarterly basis or when an employee changes position and make appropriate changes as needed. The AA data manager will make necessary changes as needed to user permissions.

The data manager at the Administrative Agency is the Local Responsible Party (LRP) and is responsible for ensuring that an individual is designated as an LRP at each service provider site. Internally, at DSHS, the HIV/STD Comprehensive Services Branch Manager is designated as the LRP. The LRP will be responsible for implementing and enforcing security and confidentiality policies and procedures and for investigating suspected breaches. Only DSHS and AA data managers have rights to ARIES Report/Export. The AA data managers must not grant ARIES Report/Export rights to any other users. The AA data managers must not grant unnecessary access to users within ARIES to run reports and export data.

AA data managers are responsible for ensuring that authorized users understand:

- 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 AA Data Managers

The AA data managers must develop local policy and procedures to implement this policy including those associated with authorization of users and authorization of user permissions according to role. Additionally, AA data managers must also develop plans for how they will ensure that ARIES user and security policies are followed by AA staff, service provider agencies, and subcontracting personnel who use ARIES.

AA data managers make certain:

- ARIES training has been complete
- Each user has an individual login and security certificate, no login names or certificates can be shared, nor should generic login names be created.
- All users prior to being given access to ARIES successfully complete confidentiality and security training, sign a confidentiality agreement that affirms individual responsibility for keeping client information and data confidential, and sign an assurance that they have reviewed security policies and procedures relevant to their position. The confidentiality and assurance agreements must be signed annually. The original must be stored in the employee’s personnel file and a copy must be maintained by the employee. The date(s) of the training(s) must be documented in the employee’s personnel file.
- Revoke the user’s rights within the ARIES system and contact DSHS staff by telephone and email to revoke user rights immediately after a user leaves employment or no longer requires access to ARIES.

8.2 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 that 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 AA staff may be released without consultation with DSHS. However, aggregate profiles of client characteristics that include cross-tabulated tables with cells that contain fewer than 10 clients 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.

9.0 Physical Security

9.1 Building Security

- All confidential information must be maintained in a secure area. No remote access is allowed. A secure area is an area that is protected by at least one level of physical security, although it is preferable that such information be maintained behind two levels of physical security. Examples of physical security levels include a secured access card reader, locked door or a security guard.
- The physical security of the building containing the confidential information must be approved by both the provider LRP and the AA data manager.

9.2 Computer Workstations

- All computer workstations with access to ARIES data must be physically located in a secure area.
- No laptops or other portable computing devices can be programmed to have ARIES access without DSHS approval and only if they abide by 12.0 & 12.1 in this document.
- Workstations with access to ARIES must be password protected at the Windows login level and have a password protected screensaver program installed and activated. The screensaver should be set to automatically activate in 5 minutes or less when the workstation is not in active use.
- Passwords must comply with DSHS-published password guidelines found at: http://online.dshs.state.tx.us/it/security/docs/passguide.doc.
- 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.
- No one should access a computer or network using another person's access without written authorization.
- Computer screens must not be readily observable by non-authorized users as they pass through the office area or approach reception desk. Security/Privacy screens must 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 or worked with on any computer that is not secure. This includes no remote access such as Go To My PC or VPN.

10.0 E-Mail

- Any client-level information or aggregate reports which could potential identify a client should not be transmitted by e-mail.
- Protected Health Information can be emailed via an attachment that is encrypted and password protected as long as the password is delivered through a phone call or in a separate email that does not contain any identifying information or the words HIV and/or AIDS.
- If a client or provider emails about their specific case, it is best practice to email the person back and ask them to call the provider directly.
- Staff should not include any identifiers within the email that pertain to HIV or AIDS, such as the program name or descriptions within their signature block.

11.0 Handling Electronic Data

11.1 Electronic Data Access

- Access to ARIES will only be granted as defined in the user policy. http://www.dshs.state.tx.us/hivstd/policy/policies/241000.pdf
- 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 AA data managers have rights to ARIES Report/Export. AA data managers must not grant ARIES Report/Export rights to any other users.
- AA data managers must ensure and monitor confidential data exported for the purpose of evaluation, monitoring, or quality assurance by the submitting agency or the AA are physically and electronically secure and disposed of properly.
- Exported confidential information for the purpose of evaluation, monitoring, or quality assurance with the AA or the submitting agency must not be taken to private residence unless specific

permission has been granted by the state LRP. Likewise, remote access of a work computer from home in order to access ARIES is prohibited.

12.0 Removable, External Storage Devices

All staff authorized to access confidential information must be individually responsible for protecting their assigned portable devices including, but not limited to: PDA, blackberries, cell phones, flash drives, diskettes, CD-ROMS, zip disks, tape backups, removable hard drives, smart cards, and/or GPS systems.

12.1 Laptops

Laptops used as work computer fall under the same confidentiality and security guidelines as indicated under section 10.0 Physical Security. 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 AA;
- DSHS approves the signed agreement;
- The laptop user has a separate signed statement indicating receipt and understanding of laptop agreement/requirements;
- The laptop is docked;
- The laptop does not leave the office; and
- The laptop does not have a wireless Internet connection.

12.2 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 password protected. Passwords must be stored separately from the device.
- When taking confidential data stored in 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 the state LRP.
- 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.

12.3 Personal Storage Devices (PDA)/Blackberries/Cell Phones

PDA, Blackberries or cell phones will not be used to access, store or transmit confidential information.

13.0 Evolving Technology

If the security guidelines specified in this policy do not cover evolving technology, it is the responsibility of the AA data managers or service provider LRP to seek the guidance of DSHS.

14.0 Revision History

Date	Action	Section
August 18, 2010	This is a new policy	all

EMPLOYEE POLICY ACKNOWLEDGEMENT FORM

ARIES Security Policy 231.001

I certify that I have read, understand, and agree to adhere to the ARIES Security Policy 231.001

I understand that Bexar County may revoke my access code or other authorized access to confidential information for any reason. My ARIES access privileges are subject to periodic review, revision, and if appropriate, renewal.

I understand that I will be held responsible for my misuse or wrongful disclosure of confidential information and for my failure to safeguard my access code/password or other authorized access to confidential information.

I understand that it is my responsibility to ask clarifying questions if I need assistance interpreting a policy.

______________________________________ ________________

Signature Date

____

Print Name

____

Agency