2011.01 Confidential Information Security

Policy Number	2011.01
Effective Date	July 2, 2008
Revision Date	May 10, 2014
Subject Matter Expert	Epi and Surveillance Specialist
Approval Authority	TB/HIV/STD Section Director
Signed by	*Felipe Rocha, M.S.S.W.*

1.0 Purpose

The purpose of this policy is to define security standards for protecting the confidential information collected and maintained by the TB/HIV/STD (THS) Section associated with surveillance, epidemiology, public-health follow-up, and the Texas HIV Medication Program and any other confidential information within the Section and its Branches. This policy addresses the administrative, physical, and technical safeguards for the security of confidential information.

This policy has been written in alignment with requirements in the Department of State Health Services (DSHS) *HIV and STD Program Operating Procedures and Standards (POPS)* (dshs.texas.gov/hivstd/pops/), the Information Security Policy (hhsconnection.hhs.texas.gov/it/information-securitycybersecurity), Computer Usage Policy IR-2202, and the Centers for Disease Control and Prevention (CDC) *Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Surveillance Programs*.

2.0 Background

In fulfilling its mission to prevent, treat and control the spread of TB, HIV, STDs and other communicable diseases, the DSHS THS Section, its contractors and external partners obtain personal and private information regarding individuals they serve. The THS Section must be vigilant in maintaining the integrity of the systems that contain this information.

3.0 Authority

V.T.C.A., Penal Code, Chapter 16, Chapter 33; V.T.C.A. Health and Safety Code, 81.046 and 81.103-81.104; V.T.C.A., Texas Government Code, Chapter 552.

4.0 Definitions

Central Office – The TB/HIV/STD Section, Department of State Health Services (DSHS) main office located in Austin, Texas.

Confidential information – Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released.

Confidentiality – The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients and research participants.

External – Entities outside of the DSHS Central Office that the THS Section contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Local Responsible Party (LRP) – An official who accepts responsibility for implementing and enforcing TB/HIV/STD Section policies and procedures related to the security and confidentiality of TB/HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information. The LRP also has the responsibility of reporting and assisting in the investigative breach process. Local Responsible Parties will be designated both internally and externally. Internally the HIV/STD/HCV Epidemiology and Surveillance Branch manager, the HIV/STD Prevention and Care Branch manager, the TB and Hansen's Disease Branch manager, and the Program Informatics Group manager will be designated as the Local Responsible Parties.

Overall Responsible Party (ORP) – DSHS official who accepts overall responsibility for implementing and enforcing TB/HIV/STD and Viral Hepatitis security standards and practices. The ORP is responsible for protecting data as they are collected, stored, analyzed, and released and must certify to CDC annually that all security program requirements are being met. The THS Section Director will be designated at the Overall Responsible Party.

Security – The protection of public health data and information systems for the purposes of (1) preventing unauthorized release of identifying public health 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. THS Section – The TB/HIV/STD Section, which includes the Health Communications and Community Engagement Group, the HIV/STD Prevention and Care Branch, the TB/HIV/STD Epidemiology and Surveillance Branch, and the TB Services Branch.

THS Section – The TB/HIV/STD Section, which includes the Health Communications and Community Engagement Group, the HIV/STD Prevention and Care Branch, the TB/HIV/STD Epidemiology and Surveillance Branch, and the TB Services Branch.

5.0 Policy

It is the policy of the DSHS THS Section that information collected to prevent, treat, and control the spread of TB, HIV, and STDs will be protected and maintained to ensure patient

confidentiality.

6.0 Persons Affected

This policy applies to all persons who may have access to confidential TB, HIV, STD and Viral Hepatitis information associated with surveillance, epidemiology, public health follow up, and the Texas HIV Medication Program. This includes the DSHS THS Section employees (permanent and temporary), IT staff, volunteers, students, and DSHS THS Section contractors.

7.0 Responsibilities

All persons affected by this policy (specified in section 6.0) are required to follow this policy and the relevant procedures associated with this policy.

- All persons must complete the following before being given access to confidential information:
  - Sign a confidentiality agreement that affirms individual responsibility for keeping client information and data confidential. The original must be stored in the employee's personnel file and a copy must be maintained by the employee. The confidentiality agreement must be signed annually, which is the *HHS Enterprise Architecture and Security Management, Security and Privacy Agreement (SPA), HIV/STD 301.002*.
  - Successfully complete confidentiality and security training. The date(s) of the training(s) must be documented in the employee's personnel file. For DSHS employees, this training will be in addition to the security awareness and security/computer usage training required by DSHS policy.
- All persons 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.
- All persons are responsible for reporting possible security risks to the LRP or ORP.
- All persons are individually responsible for protection of his/her own desk/work area, workstation, laptops or other devices associated with confidential information.
- All persons are responsible for challenging 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.
- 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.

Overall Responsible Party

- The THS Section manager will serve at the Overall Responsible Party (ORP).
- The ORP shall have final approval authority for THS Section security and confidentiality policies and procedures.
- The ORP will have overall responsibility for assuring that the TBHS Section security and confidentiality policies and procedures are implemented and enforced.

- The ORP with the LRPs will ensure that this policy is reviewed annually and that evolving technology is reviewed on an on-going basis to make certain that the program's data remains as secure as possible.
- The ORP will participate with the LRPs in the breach investigation process.
- The ORP will provide security certification to CDC or other federal funders.

Local Responsible Party

- All external sites and the Central Office must designate a Local Responsible Party (LRP).
- Internally the TB/HIV/STD Epidemiology and Surveillance, TB Services and HIV/STD Comprehensive Services Branch managers will be designated as the Local Responsible Parties.
- The LRP will approve any THS Section staff requiring access to confidential information maintained by the THS Section. The LRP will grant authorization to persons who have a work-related need to view confidential information.
- The LRP will ensure that all staff, including contractors, are trained as specified in the training requirements listed at (TB/HIV/STD Security Training Plan) and as otherwise specified by DSHS.
- The LRP will maintain a list of persons who have been granted authorization to view and work with confidential information. The LRP will review authorized user lists annually.
- The LRP will ensure that this policy is reviewed annually and that evolving technology is reviewed on an on-going basis to make certain that the program's data remains as secure as possible.
- The LRP will be responsible for re-evaluating and re-assigning access to confidential information when an employee changes position within the THS Section.

8.0 Access

Access to confidential information by program staff (central office and external staff) shall be based on their responsibilities, and should follow these guidelines:

- Data Entry – record searches, data entry
- Administrative – data management, data transfers, data imports, facility table maintenance, user account management, quality review
- Record Searches – read only
- Data Analysis for Reporting – read only

Access to confidential information by IT support staffs need to practice least-privilege access controls for rights/permissions by specific duties. Generic user accounts should not be used for day-to-day tasks or system administration. IT access should follow these guidelines:

- Firewall Support
- Desktop Support
- Network Support
- Server Support
- Security

9.0 Procedures

All external programs must maintain written procedures for maintaining the security of confidential information. Such procedures must include the elements listed in the applicable activity-specific procedures for TB/HIV/STD Surveillance, Public Health Follow-Up, the Medication Program and the Medical Monitoring Project.

External sites that do not adopt the DSHS security and confidentiality policies and procedures shall have their policies reviewed and will have security audits by the ORP or person designated by the ORP.

10.0 Revision History

Date	Action	Section
9/1/2017	Changed "TB/HIV/STD Unit" to "TB/HIV/STD Section" to reflect new program designation	-
9/3/2014	Converted format (Word to HTML)	-
4/1/2011	Amend policy to make it applicable to the entire THS Section	All
9/28/2010	Identified Security Agreement form title	Responsibilities
	Added section	Access
	Renumbered following sections to accommodate new “Access” section	Procedures, Revision History
	Added stated by policy review for sites not adopting DSHS policies and procedures	Procedures
7/2/2008	This is a new policy	N/A