TEXAS Health and Human Services | Texas Department of State Health Services

DSHS TB/HIV/STD

Local Responsible Party (LRP) HandbookV.2-2019

Amanda Sierra, TB/HIV/STD Section Security Officer.

Amanda.Sierra@dshs.texas.gov

Office: 512-206-5974

Cell: 512-574-5765

Contents

1. Objective---------- 3
2. Definitions---------- 3
3. Introduction---------- 7
4. Local Responsible Party (LRP) Responsibilities---------- 10
5. Local Responsible Party (LRP) Bi-Annual Reporting---------- 11
6. Local Responsible Party (LRP) Change Process---------- 12
7. Security Culture---------- 13
8. Section Policies and Procedures---------- 14
9. Privacy Incidents and Investigations---------- 15
   *Privacy Incident Reporting---------- 17
   * Updated Privacy Incident Reporting Procedures 19
10. Site Assessment(s)/Inspection(s)---------- 20
11. HIPAA vs. CDC---------- 21
12. Data Release---------- 23
13. DSHS Secure Network Systems and Confidential Information Access---------- 24
   *Account Requests---------- 24
   *Deactivating a User---------- 25
14. Authorized User(s) Maintenance---------- 25
15. Security and Confidentiality Training---------- 26
16. Provisional Policies---------- 29
17. Community Based Organizations (CBO)---------- 30
18. LRP Quick Reference Guide---------- 30

1. **Objective**:
   The Department of Texas State Health Services (DSHS) TB/HIV/STD Local Responsible Party (LRP) Handbook is made available to provide guidance on topics based on security, confidentiality, privacy incidents, and policies and procedures.

   Back to Contents.

2. **Definitions**

Aggregate Data: Aggregate Data refers to individual-level information that is compiled into data summaries or summary reports, typically for the purposes of public reporting or statistical analysis. Aggregate data may contain potentially identifying information, particularly if the aggregated data are very detailed or for a small subset of individuals.

Authorized Users (AU). Authorized Users are personnel that have access to TB/HIV/STD confidential information. Authorized Users should only have access to the confidential information necessary to carry out the public health functions outlined in their job duties and should only be given access to this information after signing the DSHS TB/HIV/STD Confidentiality Agreement and completing required DSHS Security Training on an annual basis. Authorized Users are to be TB/HIV/STD program staff, which may also include personnel in IT, contract staff, temporary staff, and interns. All specific job functions should be examined before giving personnel an authorized user status. **TB/HIV/STD program staff are responsible for securing confidential information from unintended disclosure to non-TB/HIV/STD staff. All documents (annual security and confidentiality training forms) should be on file with the Section Security Officer.**

Confidential Information: Any information which pertains to a person 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, including Protected Health Information and Personally Identifiable Information.

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.

Corrective Action(s): A plan that is often developed in response to an incident. This process begins with a root cause analysis that identifies underlying problems that represent a risk of future incidents.

Disciplinary Action(s): A process for dealing with job-related behavior that does not meet expected and communicated performance standards.

Intentional: An intentional act done by intention or design.

Local Responsible Party (LRP): An official who accepts responsibility for implementing and enforcing HIV/STD security and confidentiality policies and procedures related to 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 privacy incident investigation process.

Negligent: Failure to use reasonable care, including failure to do (or not to do) something that a reasonably prudent person would do (or not do) under like circumstances.

Non-TB/HIV/STD Staff. Non-TB/HIV/STD Staff are individuals (administrators, other employees, IT staff, custodial staff, interns, etc.) who are regularly in the areas where TB/HIV/STD activities are being conducted but are not specifically a part of the TB/HIV/STD program staff. These individuals can be held responsible for the unauthorized release of confidential information. All individuals must fulfill the requirements of DSHS TB/HIV/STD Security Training, along with a signed DSHS Confidentiality Agreement. **TB/HIV/STD program staff are**

responsible for securing confidential information from unintended disclosure to non-TB/HIV/STD staff. All documents (annual security and confidentiality training forms) should be on file with the Section Security Officer.

Overall Responsible Party (ORP): DSHS official who accepts overall responsibility for implementing and enforcing TB/HIV/STD 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.

Personal Identifiable Information (PII): Data or other information which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information about them known. Personal information includes, but is not limited to, information regarding a person's home or other personal address, Social Security number, driver's license, marital status, financial information, credit card numbers, bank accounts, parental status, sex, race, religion, political affiliation, personal assets, medical conditions, medical records or test results, home or other personal phone numbers, non-university address, employee number, personnel or student records and so on. CRF § 155.260 and TAC Title 521.

Privacy Incident: An incident in which confidential 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): is an individual's health information that is created or received by a health care provider related to the provision of health care by a covered entity that identifies or could reasonably identify the individual. The 18 identifiers that are considered PHI can be found in the OHRPP Guidance & Procedures: Health Insurance Portability and Accountability Act (HIPAA).

Pseudo-anonymized Data: Individual record-level data which has been stripped of personal identifiers (e.g., name, address, Social Security number) but may contain potentially identifying information (e.g., age, sex, race/ethnicity, locality information) that when combined with other information may identify an individual. If the combining of information could identify an individual, these data are considered confidential.

Rule of Fifty: The acceptable threshold for the release of aggregate TB, HIV/AIDS, STD surveillance, epidemiologic, and public health follow-up data. The underlying population of the statistic released must be a population of greater than 50 people and must also be at least twice the number of cases. The Rule of Fifty is used to protect the identity of people in very small and less populated areas; where release of this information can be linked to disease data and could reveal someone's information.

Security Team: Internally, the Security Team consists of the Section Security Officer, Group manager, and the Local Responsible Party(s) and sometimes the Overall Responsible Party (ORP) if the incident involves multiple program areas. Externally, this team consists of appropriate staff designated to serve in this team. The Security Team is responsible for investigating suspected privacy incidents, gathering all facts related to the incident, drawing conclusions, making recommendations for further action, and providing a closing report.

Section Security Officer: The Section Security Officer represents the Overall Responsible Party (ORP) to enforce security and confidentiality compliance. The duties include, but are not limited to, investigating privacy incidents, reviewing privacy incident reports, ensuring security and confidentiality compliance, security training, and inspection of facilities. The Section Security Officer serves as a resource to the LRPs when needed.

TB/HIV/STD Section: Section within the DSHS Laboratory and Infectious Disease Services Division, which includes the Health Communications and Community Engagement Group, the HIV/STD

Prevention and Care Branch, the TB/HIV/STD Epidemiology and Surveillance Branch, the TB Services Branch, and the Pharmacy Branch.

Unauthorized Release of Information. Information that is released to an unauthorized individual(s) and/or receiving information that was not intended for the individual.

Unauthorized Access of Information. Information an individual(s) had access to without proper authorization.

Violation of Confidentiality: Violation of protocol resulting in the improper disclosure of confidential information, which includes 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.

Violation 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.

Visitors: Visitors are individuals who are non-TB/HIV/STD staff and/or individuals who will be temporarily in the area of TB/HIV/STD confidential information. Visitors should sign-in and out (to access TB/HIV/STD areas, have a visitor identification (if possible), and should be escorted by an authorized staff member at all times. **TB/HIV/STD program staff are responsible for securing confidential information from unintended disclosure to and/or of visiting individuals.**

Back to Contents.

3. Introduction

The LRP Handbook will undergo annual review with the latest version serving as the main reference source for LRPs in Texas. As with any set of policies and procedures, some issues may not be identified until they are put into practice. Accordingly, requirements will be updated as it becomes necessary. A current version of the LRP handbook will be available on the DSHS TB/HIV/STD website.

The LRP Handbook provides a guidance for LRP(s) to ensure TB/HIV/STD security policies and procedures are implemented and enforced to protect confidential information for their organization. DSHS TB/HIV/STD Section security policies are primarily derived from the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Program (2011) by the Centers for Disease Control and Prevention (CDC).

DSHS TB/HIV/STD Section understands that this responsibility may come as an additional duty. Our goal is to assist you in this responsibility and create a strong working relationship with LRPs across the state. We are all working together to meet the same goal of taking care of the protected health information (PHI) of the citizens of Texas. If there are any questions, concerns, comments, or complaints do not hesitate to contact the Section Security Officer at DSHS.

Local Responsible Party (LRP): An official who accepts responsibility for implementing and enforcing HIV/STD security and confidentiality policies and procedures related to 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 privacy incident investigation process.

Overall Responsible Party (ORP) at Section. DSHS official who accepts overall responsibility for implementing and enforcing TB/HIV/STD 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. The ORP is also responsible for having an ongoing review of technology and security standards as technology changes.

Agencies that receive direct funding from CDC may have their own ORP in addition to the DSHS ORP.

Security Team: Internally, the Security Team consists of the Section Security Officer, Group manager, and the Local Responsible Party(s) and sometimes the Overall Responsible Party (ORP) if the incident involves multiple program areas. Externally, this team consists of appropriate staff designated to serve in this team. The Security Team is responsible for investigating suspected privacy incidents, gathering all facts related to the incident, drawing conclusions, making recommendations for further action, and providing a closing report.

Section Security Officer: The Section Security Officer represents the Overall Responsible Party (ORP) to enforce security and confidentiality compliance. The duties include, but are not limited to, investigating privacy incidents, reviewing privacy incident reports, ensuring security and confidentiality compliance, security training, and inspection of facilities. The Section Security Officer serves as a resource to the LRPs when needed.

Authorized Users (AU). Authorized Users are personnel that have access to TB/HIV/STD confidential information. Authorized Users should only have access to the confidential information necessary to carry out the public health functions outlined in their job duties and should only be given access to this information after signing the DSHS TB/HIV/STD Confidentiality Agreement and completing required DSHS Security Training on an annual basis. Authorized Users are to be TB/HIV/STD program staff, which may also include personnel in IT, contract staff, temporary staff, and interns. All specific job functions should be examined before giving personnel an authorized user status. **TB/HIV/STD program staff are responsible for securing confidential information from unintended disclosure to non-TB/HIV/STD staff. All documents (annual security and confidentiality training forms) should be on file with the Section Security Officer.**

Non-TB/HIV/STD Staff. Non-TB/HIV/STD Staff are individuals (administrators, other employees, IT staff, custodial staff, interns, etc.)

who are regularly in the areas where TB/HIV/STD activities are being conducted but are not specifically a part of the TB/HIV/STD program staff. These individuals can be held responsible for the unauthorized release of confidential information. All individuals must fulfill the requirements of DSHS TB/HIV/STD Security Training, along with a signed DSHS Confidentiality Agreement. **TB/HIV/STD program staff are responsible for securing confidential information from unintended disclosure to non-TB/HIV/STD staff. All documents (annual security and confidentiality training forms) should be on file with the Section Security Officer.**

NOTE: Non-TB/HIV/STD staff who perform duties with TB/HIV/STD information must meet the same documentation and training requirements as an Authorized User. While any staff may take the DSHS TB/HIV/STD Data Security and Confidentiality training, only those staff requiring access to TB/HIV/STD data should actually be granted access.

IMPORTANT: The LRP and agency are responsible for determining if an employee's "other duties as assigned" clause can be used as justification to give that employee access to confidential information. As a rule, agencies should always follow the principle of least privilege, only providing access to those employees who need it to carry out their job duties. If you have questions about whether an employee should be granted access, contact the Section Security Officer.

Back to Contents.

4. Local Responsible Party (LRP) Responsibilities

The LRP will have the responsibility of maintaining the security of confidential information for their organization as described in the DSHS TB/HIV/STD Security Policies and Procedures. The LRP will approve the authorization of users to have access to confidential information and will request access for any DSHS-approved secure network database.

The LRP and/or their designee will ensure security and confidentiality training for new and current employees, perform and submit bi-annual reports, maintain records of all current confidentiality agreements and

training certifications, investigate privacy incidents, and perform corrective and disciplinary actions as needed. ***All forms are subject to audit***. The LRP should be in a position of authority to perform these functions, as they serve as the responsible party for their authorized users.

LRP Duties and Responsibilities.

(1) Maintain a list of all personnel that are authorized to access confidential information
(2) Maintain all copies of current confidentiality forms and training certificates.
(3) Inform DSHS when an Authorized User (AU) needs to have access terminated (voluntarily or non-voluntary)
(4) Ensure employees complete/renew Security Training on an annual basis
(5) Ensure employees submit a signed Confidentiality Agreement on an annual basis (submitted with security training renewal to the Section Security Officer).
(6) Send Bi-Annual Reports to TB/HIV/STD Section Security Officer along with AU list (or Health Communications Manager if security officer position is vacant).
(7) Investigate privacy incidents and complete privacy incident reports within 24 hours of discovering incidents (with updates as the investigation/information becomes available).
(8) For any individual(s) potentially implicated in a privacy incident, limit or restrict access to confidential information for the implicated individual(s) until the privacy incident investigation is complete
(9) Consult with the TB/HIV/STD Section Security Officer about privacy incidents, as needed
(10) Establish and/or enforce corrective or disciplinary actions in conjunction with agency management when needed
(11) Ensure organizational policies are in line with DSHS TB/HIV/STD Security policies
(12) Provide validation of access requests for DSHS databases for agency AUs

Instructions for requesting access to DSHS databases, terminating user access to DSHS databases, and completing security training and confidentiality agreement requirements/annual renewals can be found at the DSHS TB/HIV/STD Security and Database Account Management website.

Back to Contents.

5. LRP Bi-Annual Reporting

i. **LRP Bi-Annual Reports.**
Reporting is done biannually. The report is derived from the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Program (2011) by the Centers for Disease Control and Prevention (CDC). The report can be found online, and your electronic signature will be accepted. The Bi-Annual reports support LRPs on multiple aspects of their agency and assist DSHS to evaluate if an agency may need additional support.

LRP Bi-Annual Security Review Checklist Instructions

LRP Security Review Questionnaire

Bi- Annual Reports Submission Dates

Period	Time	Due Date	Documents to Submit
1st	July 1 – December 30	December 31	DSHS Security Review Questionnaire & Authorized User List
2nd	January 1—June 30	July 1	DSHS Security Review Questionnaire

Back to Contents.

6. LRP Change Process

i. An LRP who is relinquishing the position should notify the DSHS TB/HIV/STD Section Security Officer at least two weeks **before** the date of relinquishment. To make the transition of duties official, the departing LRP should forward the name, email, and phone number of the new LRP and acknowledge that the LRP roles and responsibilities have been discussed with the new LRP. The new LRP and the TB/HIV/STD program-level director or higher responsible agency

official should be copied/included in this correspondence to the Section Security Officer.

ii. If the departing LRP is no longer available to make this acknowledgment, a TB/HIV/STD program-level director or higher responsible agency official will need to send an email **within one week** of the relinquishing LRP leaving to confirm the items listed in the above section.

NOTE: All LRP change processes/questions should be communicated to TBHIVSTD.AccountRequests@dshs.texas.gov within the noted time above.

Back to Contents.

7. Security Culture

DSHS TB/HIV/STD Section wants all employees and contractors to develop a constructive and collaborative security culture. Aside from the laws in place that dictate security practice, we need to remember we are protecting someone's private life. To simplify security practices, we have summarized security into three parts of a privacy incident and three questions to be asked to determine if an unauthorized access and/or release has occurred.

i. Three Components of a Privacy Incident.

When gathering information to determine if a privacy incident has occurred, it is helpful to consider if three basic components are present:

a. Confidential information (e.g., health status, test results, etc.)
b. Identifying information (e.g., name, Social Security number, etc.)
c. A means to access or expose information (e.g., database, paper records, word of mouth, etc.)

ii. Privacy Incident Defined.

Privacy Incident. A privacy incident is which confidential information might have been divulged to unauthorized parties and/or protocol for handling of confidential information might not have been followed. Privacy incidents can be intentional or negligent.

Intentional. This is an intentional act done by intention or design, such as an angry patron that takes a file and runs out.

Negligent. Failure to use reasonable care, including failure to do (or not to do) something that a reasonably prudent person would do (or not do) under like circumstances. **iii. Types of Privacy Violations.**

(1) Violation of Confidentiality. A violation of confidentiality occurs when secure handling protocol for confidential information was not followed, and confidential information was divulged to unauthorized parties (i.e., sending an email with client PHI to the wrong individual).

(2) Violation of Protocol. A violation of protocol occurs when the secure handling protocol for confidential information was not followed (i.e., sending PHI through email).

Back to Contents.

8. Section Policies and Procedures

The LRP is expected to be familiar with the security policies and applications of these policies within of their own agency and within the DSHS TB/HIV/STD section. The LRP serves as the resource to their employees and the Section Security Officer serves as the resource to the LRP. LRPs should have a solid understanding of what the policies require. When in doubt, the LRP should consult with the Section Security Officer. If policies are unclear to you, they may be unclear to others in your agency.

i. Policies and Application.

Successful application of security policies takes practice. Your understanding of security policies and how they apply to your agency will become more developed as you investigate privacy incidents, submit privacy incident reports, complete biannual LRP reports, and conduct inspections of your agency facilities. The LRP reporting process was created to help LRPs develop a step-by-step understanding of each policy and procedure by learning how to remediate any identified deficiencies. When needed, site inspections by

the Section Security Officer can provide an additional pair of eyes, which provides the opportunity to recognize items you may have missed.

ii. **Agency Policy vs. DSHS Security Policies.**
A local agency may have stricter policies than DSHS. We do not wish to confuse the two, nor do we wish to stop an agency from having additional security measures. In training, if there is mention of what is required by DSHS, the LRP needs to mention if the agency's policy is different or how it goes beyond the DSHS security policies. Agency security policies **cannot be less restrictive** than DSHS TB/HIV/STD Section security policies.

DSHS TB/HIV/STD Security Policies and Procedures.

Laws, Rules, and Authorizations.

Back to Contents.

9. Privacy Incident(s) and Investigations

Privacy incidents are going to occur. The primary goal of the incident reporting process is to identify the root cause(s) and remediate those causes so similar incidents are less likely to occur in the future. Ideally, we want to focus on corrective actions. Corrective actions don't have to be synonymous with disciplinary actions, particularly in cases where there is no negligence or malice on the part of an employee. **DSHS reserves the right to remove a non-DSHS employee's access to DSHS-owned applications as a result of privacy incident(s).** The decision to discipline a non-DSHS employee implicated in a privacy incident is left to that employee's agency. All corrective and disciplinary actions taken as a result of a privacy incident should be documented in the privacy incident report submitted to DSHS.

i. **Privacy Incident Reports**
A privacy incident report should be submitted within 24 hours of discovering an incident. The most important part of the privacy incident reports are the narratives. This provides a clear understanding to what has occurred and how to choose the appropriate corrective

actions. Some privacy incidents will be clear and require simple corrective actions, others will not. You may have to submit additional follow-up information after submitting the initial report.

To report a suspected privacy incident, use the DSHS TB/HIV/STD Section Privacy Incident Report. **NO PHI/PII should be reported in the report.**

ii. **Privacy Incident Defined.**

a. ***Refer to Section 7 (ii.1).***

iii. **Types of Data Compromised.**

a. **Personal Identified Individual (PII) Record-Level Data.**
Information which, when combined with other information, could potentially identify an individual(s). This includes, but is not limited to, such information as medical record/case numbers, demographics, or locality information that describe a small subset of individuals, where the Rule of Fifty should always be followed (e.g., block data, zip codes, race/ethnicity).

b. Pseudo-anonymized Data.
Individual record-level data which has been stripped of personal identifiers (e.g., name, address, Social Security number) but may contain potentially identifying information (e.g., age, sex, race/ethnicity, locality information) that when combined with other information may identify an individual. If the combining of information could identify an individual, these data are considered confidential.

c. Aggregate Data.
Aggregate Data refers to individual-level information that is compiled into data summaries or summary reports, typically for the purposes of public reporting or statistical analysis. Aggregate data may contain potentially identifying information, particularly if the aggregated data are very detailed or for a small subset of individuals.

iv. **DSHS Types of Privacy Incidents.**

a. ***Refer to Section 7 (iii).***

v. **Unauthorized Incidents.**

a. **Unauthorized Release of Information.** Information that is released to an unauthorized individual(s) and/or receiving information that was not intended for the individual.

b. **Unauthorized Access of Information.** Information an individual(s) had access to without proper authorization.

vi. Describing the Privacy Incident.

The narrative is the most important part of the privacy incident form; the more details, the better. If critical details are missing in the initial report, the Section Security Officer will need to follow up with the agency's LRP to obtain these details.

vii. Describe Contributing Causes to the Privacy Incident.

The goal is to get insight as to why this privacy incident occurred. Contributing causes can be a symptom of a larger problem, or it can be an isolated event.

viii. Confidential Information Compromised.

Description of the information potentially compromised. (i.e., a file of TB patients with names, addresses, etc.).

xi. Disciplinary or Corrective Actions.

Document all corrective or disciplinary actions taken here. Remember, corrective action should not be synonymous with disciplinary action. Not all incidents will require disciplinary action to be taken, but all will require some form of corrective action.

xii. Privacy Incident Investigations.

The purpose of the investigation is to understand what type of information has been comprised, how many people whose PHI has been compromised by the incident, how the incident occurred, and how similar incidents can be prevented in the future. It is helpful to think of privacy incidents as an opportunity to fix security gaps in your agency before a more serious privacy incident occurs. The privacy incident investigation may provide insight into problems related to technology, training, communication, workflow, policy, employee morale and/or other factors. Remember, if one employee is confused or frustrated by security compliance, it's likely that others are, too.

a. <u>What happens when a Privacy Incident Investigation Occurs?</u>

1. **Obtain or create a privacy incident report of what has occurred.** This documentation may be used to complete the privacy incident report submitted to DSHS. In reviewing the report, it is good to fall back to the three components of a privacy incident. The questions on the privacy incident form will also help guide your investigation.

   ***Questions with unknown, unclear, or ambiguous answers should always warrant more questioning until they lead to a solid answer. When in doubt, ask for assistance from the Section Security Officer.

2. **Submit the Privacy Incident Report.**
   If the situation is "**simple**", the LRP may submit a privacy incident report, describe the corrective and/or disciplinary actions, and the case will be closed out.
   <u>Simple Incident Example:</u> *An encrypted email containing PHI of one individual was erroneously sent to the wrong health department employee. Corrective actions will be sent to agency.*

   For more "**complex**" issues, the Section Security Officer may inform the DSHS Overall Responsible Party. If clarifying information is needed, the Section Security Officer will ask for it. The emphasis is a team effort to resolve the situation.
   <u>Complex Incident Example 1:</u> *An encrypted email containing PHI of 500 or more individuals sent to an unauthorized individual. This privacy incident would have to be reported to the U.S. Department of Health and Human Services Office of Civil Rights.*
   <u>Complex Incident Example 2:</u> *An employee with access to PHI deliberately revealed the name and health status of an individual to an unauthorized party.*

3. **Submission to the Texas Health and Human Services Commission Privacy Officer and Legal Department.** All privacy incidents will be reviewed by the Section Security Officer and then submitted to Texas Health and Human Services Commission (HHSC) Privacy Officer and Legal Department, if warranted.

4. **Determinations of Privacy Violations.** The HHSC Privacy Officer and Legal Department will make the final determination if a privacy violation has occurred. The LRP will be contacted with the **final** DSHS Privacy Office determination, disciplinary and/or corrective actions, and additional steps, if needed. If it is determined that a breach has occurred, you may be instructed to the report the breach to the U.S. Department of Health and Human Services' Office of Civil Rights and/or notify the individuals(s) affected by the breach.

b. Updated Privacy Incident Reporting Procedures

Process for Individuals Reporting Privacy Incidents

1. Immediately report Privacy Incident to upper management and/or Local Responsible Party
2. Complete the DSHS TB/HIV/STD Section Privacy Incident Report (within 24 hours of discovery) and submit to the Section Security Officer
    - TB/HIV/STD Section Security Officer will follow-up, if needed.

Section Security Officer Procedures

2. TB/HIV/STD Section Security Officer will follow-up, if needed
3. Report to DSHS Privacy Office

***Based on Determination/Privacy Incident, Corrective Actions/Steps are issued

- Further Investigation
- Re-training (individual staff and/or all staff)
- Report to U.S. Health and Human Services Office of Civil Rights, (if required)
- Notify individual/s who were affected (if required) within 60 days on agency/business letterhead (including notification to DSHS Privacy Office when this occurs)

Important to DSHS Internal and External Site(s): All privacy incidents will have a determination made by either the DSHS Privacy Office or the agency's own privacy/security leadership as noted below:

- **DSHS Internal**—Section Security Officer will report to DSHS Privacy Officer immediately

- **DSHS External**—Section Security Officer will follow up with external site. External site(s) will be **required** to conduct an investigation on the privacy incident and provide a determination of what type of violation occurred to the Section Security Officer within an allotted time frame.

For more information, please contact the Section Security Officer.

Breach of Confidentiality Response Policy.

DSHS TB/HIV/STD Section Privacy Incident Report

Back to Contents.

10. Site Assessment(s)/Inspection(s)

a. Security Risk Assessment

A Security Risk Assessment is an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of confidential information." Conducting a security risk assessment is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementations of the TB/HIV/STD section. The Security Risk Assessment requires entities to implement reasonable and appropriate security measures to protect against reasonably anticipated threats and/or hazards to the security of the TB/HIV/STD Section. Security Risk Assessments are conducted yearly and/or as needed basis. Security Risk Assessments can be on-site visitations and/or review of LRP Bi-Annual Report Summary.

1. **How are Security Risk Assessments conducted?**
   Security Risk Assessments typically examine seven key security components, including: Administrative Safeguards, Physical Security, Technical Safeguards, Organizational Standards, Policies and Procedures, LRP Documentation, and Privacy Incidents.

   Each security component will have varied security measures and will be rated by individual agency. An individual agency's rating

will depend if the security measure is in effect and/or a suitable option for the security measure is in place (i.e., proximity card access instead of passcode entry).

If an agency is evaluated as being a security risk, corrective actions and/or control measures will be issued.

Security Risk Assessment

b. Inspections

On-site inspections can occur at any time DSHS Security Team deems a site visit is needed. Agencies will have prior notification to arrival. There will be several steps prior to on-site inspections as outline below:

1. Notification (by phone and/or email) to the agency of an on-site inspection from the Security Team
2. Request a copy of the current Authorized User List, the agency's security and confidentiality policies and/or procedures, and the agency's IT Certificate (IT certificate to be completed and signed by the agency's IT staff). *Must be received at least 30 days, if applicable, prior to visit by the Section Security Officer/Team*
3. Security Team will review all agency information (Authorized User List, Agency's security and confidentiality policies and/or procedures, IT Certificate, and Privacy Incident Reporting)
4. A copy of the site's assessment will be provided to the organization following the inspection within fourteen (14) calendar days.

Back to Contents.

11. HIPAA vs CDC

i. Protected Health Information (PHI) vs. Personally Identifiable Information (PII)

Comparing what is Protected Health Information (PHI) vs. Personally Identifiable Information (PII) can be confusing because both are *Individually Identifiable Health Information*. It is the context of the use of this information that determines if it is PHI or PII. For HIPAA to be

applicable, there are only three rules to determine if the person and/or organization is a covered entity because of healthcare activities.

Outside of HIPAA, confidential information falls under PII CFR 200.79 which states that *the definition of PII is not anchored to any single category of information or technology*. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. CRF § 155.260 and TAC Title 521 are the laws that govern protection of PII. The CDC refers to confidential information as PII and not PHI in the Data Security and Confidentiality Guidelines.

ii. Determination of Covered Entity Based on Three Rules.

a. Hybrid Entity - Covered Entities can fall into what is called a Hybrid Entity. This means that part of the organization performs healthcare activities and the other part does not. DSHS is considered a Hybrid Entity. A Hybrid entity can separate its healthcare activities to be covered under HIPAA and the remaining operations to fall under the applicable privacy laws. This means that some privacy incidents will be considered a violation under HIPAA because of the context of the use of *Individually Identifiable Health Information*, while some will not. Any organization has the authority to declare themselves a Hybrid Entity under the Privacy Rule.

1. HIPAA (Covered Entities)

- *Healthcare Provider* - A provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
- *Health Plans* - With certain exceptions, an individual or group plan that provides or pays the cost of medical care. The law specifically includes many types of organizations and government programs as health plans.
- *Healthcare Clearinghouse* – An entity involved in the transmission of health information in electronic format for various transactions. This doesn't include public health surveillance.
- *Health Care* - Care, services, or supplies related to the health of an individual, including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of

the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

2. **CDC (Non-HIPAA)**
   - *Surveillance* is monitoring of behavior, activities, or other changing information for the purpose of influencing, managing, or protecting people. *Individually Identifiable Health Information* not used for healthcare activities now becomes PII.
   - Contractors to the CDC (DSHS) report privacy incidents of PII directly to the CDC. All other organizations fall back the privacy laws regarding PII.
   - Surveillance data will be transmitted according to standards outlined in the DSHS TB/HIV/STD policies and procedures.
   - *PII utilization and usage should follow the stricter of security and confidentiality standards.*

3. **Dual Roles (Surveillance/Clinical)**
   Situations where personnel serve in dual roles can create confusion. Staff in these roles should generally adhere to the stricter set of standards that apply to the job function they are performing. It is critical for staff to understand that surveillance work is not patient care.

   NOTE: Having access to patient care records is not the same as access to surveillance data. Some electronic medical records platforms have the capability to pull surveillance data for submission, but each employee should not have the same type of access. The goal is to have the minimum number of authorized users necessary to carry out public health functions. Designating all staff as authorized users will not be accepted.

Back to Contents.

12. Data Release

The LRPs will have access to reporting databases, such as THISIS. Access to your areas database is readily available and you are entitled to that information. Provisional data is not recommended for release and should be kept "frozen" until it is processed for public distribution. Releasing provisional data that is in conflict with DSHS dissemination can cause controversy, distrust, and even panic among the citizens of Texas.

Data Release Policy.

Back to Contents.

13. DSHS Secure Network Systems and Confidential Information Access

There is a strict policy on handling requests for access to DSHS Secure Network Systems and confidential information. All steps are to be followed and all required documentation must be received in order to create an account for you.

i. Account Request Forms.

The account request procedure and security training documentation was extensively revised in February 2019. **All requested documents must be provided to TBHIVSTD.AccountRequests@dshs.texas.gov.**

Following this process will ensure both the LRP and DSHS have required documentation from employees prior to access approval.

a. Steps for Account Access

The following steps apply for ALL DSHS database account requests. Please read carefully and follow directions as described. Requests for access to a database must come from the Local Responsible Party (LRP) and/or DSHS-approved LRP designee for your agency. ***DSHS WILL NOT ACCEPT ANY REQUESTS WITHOUT APPROVAL FROM AN LRP AND/OR LRP DESIGNEE.***

1. **Complete Annual Security Training**

a. Certificate should be saved as Lastname_Firstname_Agency_Strn.pdf

2. Complete **Account Request form**
   a. Please fill out form electronically. **Please do not submit scanned copies of this document.**
   b. Save form as Lastname_Firstname_Agency_AccRq.pdf

3. Complete and Sign **Confidentiality Agreement**

a. The Confidentiality Agreement must be completed in Adobe Reader. Completing the agreement in Chrome or another web browser window will prevent you from signing the form.
b. Save form as Lastname_Firstname_Agency_CON.pdf

4. Complete and Sign **Acceptable Use Agreement form**
   a. Save form as Lastname_Firstname_Agency_AUA.pdf
   b. Saving and sending only page 7 of this document will be accepted

5. Attach and email ***all completed*** required documents to your LRP and/or DSHS-Approved LRP designee. Let them know they need to sign in the spot for LRP signature on the Account Request form and forward **all *four*** documents to TBHIVSTD.AccountRequests@dshs.texas.gov.

6. Save all documents for future use.

b. Deactivating User from DSHS Secure Network Systems

A supervisor and/or LRP is responsible for notifying the DSHS TB/HIV/STD Section when an employee ends employment with the agency and/or changes to a new department/role that will no longer require the individual to access the DSHS Secure Network Systems(s).

1. Complete the **Account Deactivation Request Form** to deactivate an account
2. Email the completed form TBHIVSTD.AccountRequests@dshs.texas.gov
3. Save all documents for your records

Please see the following link for the most up-to-date procedures and forms.

DSHS TB/HIV/STD Security and Database Account Management

Back to Contents.

14. Authorized User(s) Maintenance

A list of Authorized Users needs to be maintained by the LRP and/or designee. Due to the large numbers of personnel) who have access to confidential statewide records, users need to be documented in a uniform manner. An Excel spreadsheet will be provided in the approved format. **This spreadsheet will need to be emailed to the Section Security Officer at the <u>end of the year</u> (Due on December 31, annually) and is <u>subject to random auditing</u>**.

i. **<u>Authorized Users List Spread Sheet.</u>**

Column A -Last Name
Column B -First Name
Column C -Site (First Name, initials, e.g. AustinHD)
Column D -Email
Column E -Telephone Number
Column F -Date of Security Training
Column G -Date Confidentiality Agreement
Column H -Date of Acceptable User Agreement
Column I -TxPHIN (approved or removed user)
Column J -Date Removed (from TxPHIN)
Column K -**THISIS** (approved or removed user)
Column L -Date Removed (from THISIS)
Column M -**ARIES** (approved or removed user)
Column N -Date Removed (from ARIES)
Column O -**eHARS** (approved or removed user)
Column P -Date Removed (from eHARS)
Column Q -CITRIX (approved or removed user)
Column R -Date Removed (from CITRIX)
Column S -TB GIMS (approved or removed user)
Column T -Date Removed (from TB GIMS)
Column U -VPN (approved or removed user)
Column V -Date Removed (from VPN)
Column W -**GlobalSpace** (approved or removed user)
Column X- Date Removed (from GlobalSpace)
Column Y -Other Database (state database and date)
Column Z -Other: Date Approved
Column AA -Other: Date Removed
Column AB- Privacy Incidents (Date, only if responsible for a Privacy Incident)
Column AC: Notes:

******<u>All authorized users for TB/HIV/STD Section should be included in the spreadsheet.</u>***

Authorized User List

Back to Contents.

15. Security and Confidentiality Training

Security and Continentality training is required when any individual will newly access confidential TB/HIV/STD and Viral Hepatitis information associated, but not limited to, surveillance, epidemiology, public health follow-up, and the Texas HIV Medication Program (such as new employees and/or employees with new job duties). **After this initial training**, security and confidentiality **training is required**, at a minimum, **once a year for all individuals. Certificates must be submitted to the Section Security Officer within 7 days of completion to TBHIVSTD.AccountRequests@dshs.texas.gov.** This requirement includes employees (permanent and temporary), IT staff, volunteers, students, and contractors.

The goal of security and confidentiality training is ensuring adherence to and understanding of DSHS TB/HIV/STD Section security policies. Training options will be provided in 2 forms. *In-class training that was previously provided by the Section Security Officer has been discontinued due to the high number of sites. The DSHS TB/HIV/STD Section continues to explore alternate arrangements to the in-class trainings previously offered.*

Training Options.

1. **Train the Trainer.**
   Train the Trainer option are for agencies who wish to accomplish this training requirement in-person and/or develop an agency owned-online training module (which will cover, at a minimum, DSHS required curricula. The agency will need to request a training package from the Section Security Officer at least one-month prior to training. **Requests for training packages can be made to TBHIVSTD.AccountRequests@dshs.texas.gov** with the subject line "**Request Security Training Package**".

   a. **Requirements for Train the Trainer**

1. Adhere to all required forms and requirements **TBHIVSTD.AccountRequests@dshs.texas.gov.** At a minimum, DSHS required curricula should be included.
2. Provide documentation of individuals who completed trainings (i.e., sign-in sheets and/or certificate of completion, and excel sheet with Last Name, First Name, Agency email, Site, Agency Address, and Agency ZipCode.)

Security Training Worksheet

Data Security and Confidentiality Request

Required documentation should be **received by the Section Security Officer within 30** days of completed training (for large group of trainees). If more time is needed, contact the Section Security Officer.

If documentation is not received by the Section Security Officer within the allotted time, acceptance may be contingent upon the current training available. For more information, please contact the Section Security Officer.

b. How to request Train the Trainer Materials.

1. **Submit a request at least 30 days before the proposed training date at** DSHS TB/HIV/STD Security and Confidentiality Training Request Form.
2. **Register for a GlobalScape Account.** Instructions for Requesting a GlobalScape Account**.**
    a. **Documents needed for a GlobalScape Account**
        i. Lastname.Firstname EFT Request Form
        ii. HHS Acceptable Use Agreement Form
        iii. Confidentiality Agreement Form

Note: It may take several days before your account is created. When your account is created, you will receive

notification from HHS. **Instructions for uploading files will be sent to you when you return the forms.**

c. After training is completed.

1. Upload the completed sign-in sheets and confidentiality agreement forms from individuals who attended the course in excel form, see above for requirements.
2. Send an email to TBHIVSTD.AccountRequests@dshs.texas.gov with the subject **"Trainer the Trainer Course completion, *Site Name*, *Training Date*".**
3. Email will be sent to individuals who completed the Train the Trainer course via TxTrain. Certificates will be available for download via the TxTrain website.

7. TxTrain.

Refer to the document titled, "**Instructions for completing this course**". Follow appropriate instructions depending on if an individual is a NON-HHS Employee or HHS Enterprise Employee.

TrainTx

Back to Contents.

16. Provisional Policies

DSHS TB/HIV/STD security policies cannot cover every situation, technology, or workflow. To address these emerging matters, we have created a new protocol for LRPs to follow. Any new workflow, technology, or methodology not covered by existing DSHS TB/HIV/STD Section security policy and/or procedure must be reviewed and approved by the Section Security Officer prior to implementation. The following information is needed for review:

- Agency information
- Description of new method and business need
- Explanation of how new method is not covered by current policy/procedure

- Proposed changes to current policy/procedure to ensure new method is covered
- A risk analysis of the new method and plan to mitigate risk
- Documentation supporting HIPAA and CDC compliance

IMPORTANT: Approval of the new method may be contingent upon provisions set by the Section Security Officer. Use of new method without prior approval will be in violation of the security policies and will be treated accordingly. Consult the Section Security Officer if you have any questions about this.

Back to Contents.

17. Community Based Organizations (CBO)

Community Based Organizations that do not contract with DSHS **have to** comply with the Security and Confidentiality Standards, at a minimum. It is highly recommended that these standards are met as a means of protecting confidential information. If you are a DSHS-funded CBO, contact the Section Security Officer and inform of your status. The DSHS requirements for CBOs are the following:

1) Security Training is completed annually by all CBO personnel and filed with the Section Security Officer within seven (7) days of completion.
2) Confidentiality Agreements are signed annually by all CBO personnel and filed with the Section Security Officer within seven (7) days of completion.
3) A LRP is established at the CBO to serve as a point of contact for privacy incidents and investigating privacy incidents, refer to Section 2. Local Responsible Party (LRP) Responsibilities.
4) Maintains a spread sheet of all Authorized Users, refer to Section 10. Required Documentation.

Back to Contents.

18. LRP Quick Reference Guide

CONTACT INFORMATION
DSHS Section Security Officer
Amanda Sierra, MPH
amanda.sierra@dshs.texas.gov

Office: 512-206-5974
Cell: 512-574-5765

LRP/LRP DESIGNEE RESPONSIBILITIES

- Maintain a list of all personnel that are authorized to access confidential information
- Maintain all copies of current confidentiality forms and training certificates
- Inform DSHS when an Authorized User (AU) needs to be terminated (*voluntarily or non-voluntary*) by submitting a Deactivation Request Form
- Ensure employees complete/renew Security and Confidentiality Training on an annual basis
- Ensure employees submit a signed Confidentiality Agreement on an annual basis (*submitted with security training renewal to the Section Security Officer*) **within seven (7) days of completion**
- Send **Bi-Annual Reports** to TB/HIV/STD Section Security Officer along with AU list (*or Health Communications Manager if security officer position is vacant*)
- Investigate privacy incidents and complete **initial** privacy incident reports **within 24 hours of discovering incidents** (*with updates as the investigation/information becomes available*)
- For any individual(s) implicated in a privacy incident that is potentially intentional or negligent in nature, immediately limit or restrict access to confidential information for the implicated individual(s) until the privacy incident investigation is complete
- Consult with the TB/HIV/STD Section Security Officer about privacy incidents, if needed
- Establish and/or enforce corrective and/or disciplinary actions in conjunction with agency management when needed
- Ensure organizational policies are in line with DSHS TB/HIV/STD Security policies and procedures
- Provide validation of access requests for DSHS-approved secure network systems

PRIVACY INCIDENT REPORTING

- Complete All Questions in the Privacy Incident Report.
- Contact the Section Security Officer for guidance, as needed.

DSHS TB/HIV/STD Section Privacy Incident Report

POLICIES AND PROCEDURES

- DSHS TB/HIV/STD Security Policies and Procedures
- Breach of Confidentiality Response Policy
- Data Release Agreement

BI-ANNUAL REPORTS SUBMISSION

Period	Time	Due Date	Documents to Submit
1st	July 1 – December 30	December 31	DSHS Security Review Questionnaire & Authorized User List
2nd	January 1—June 30	July 1	DSHS Security Review Questionnaire

FORMS (REQUIRED ANNUALLY)

- Confidentiality Agreement
- Acceptable Use Agreement Form
- Security Training Course
    - TrainTx Send pdf copy of certificate (*along with confidentiality agreement form*) to Section Security Officer and LRP
    - Instructions for completing the Security Training Course

IMPORTANT: **DO NOT SAVE ANY FORMS**. Instead, **BOOKMARK** the DSHS TB/HIV/STD Security and Database Account Management Page for the most up-to-date instructions and forms.

RESOURCES

- DSHS TB/HIV/STD website
- DSHS TB/HIV/STD Security Policies and Procedures
- Laws, Rules, and Authorizations
- Data Release Agreement
- DSHS TB/HIV/STD Security and Database Account Management
- Breach of Confidentiality Response Policy
- DSHS TB/HIV/STD Section Privacy Incident Report
- HIPAA Basics for Providers
- National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Program (2011)

Back to Contents.

****This handbook is subject to change without notice. For the most current version, please visit DSHS TB/HIV/STD Section Security Policies and Procedures website.*