LOCAL RESPONSIBLE PARTY HANDBOOK

TEXAS
Health and Human Services

Texas Department of State Health Services

Barbara Jennings

HIV/STD Section Privacy Coordinator

Barbara.Jennings@dshs.texas.gov

Cell: 737-281-9172

Contents

I. Objective

The Department of Texas State Health Services (DSHS) Local Responsible Party (LRP) Handbook provides guidance on security, confidentiality, privacy incidents, and policies and procedures.

II. Definitions

Aggregate Data: Individual-level information 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): Staff with access to confidential HIV, STD, or TB information. Authorized Users should only have access to confidential information necessary to carry out the public health functions required by their job duties and should only be given access to this information after signing the TB/HIV/STD Confidentiality Agreement and completing the required DSHS Security and Confidentiality training annually. Authorized Users must be HIV, STD, or TB program staff, which may also include staff in IT, contractors, temporary staff, and interns. HIV, STD, and TB program staff are responsible for securing confidential information from unintended disclosure to non-HIV, STD, or TB staff. All security documents should be on file with the Section Privacy Coordinator.

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 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.

HIV/STD Section: Section within the DSHS Laboratory and Infectious Disease Services Division.

Intentional: An act done by intention or design.

Local Responsible Party (LRP): An official responsible for implementing and enforcing HIV, STD, and TB security and confidentiality policies and procedures related to HIV, STD, or TB surveillance; epidemiology; public health follow-up; and medication program data and information. The LRP also reports and assists in the privacy incident investigation process.

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

Non-HIV/STD/TB Staff: Non-HIV/STD/TB staff are individuals (administrators, IT staff, custodial staff, interns, other employees, etc.) who are regularly in areas where HIV, STD, or TB activities are being conducted but are not HIV, STD, or TB program staff. These individuals can be held responsible for the unauthorized release of confidential information. All individuals must complete required DSHS Security and Confidentiality training annually and sign the TB/HIV/STD Confidentiality Agreement. HIV/STD and TB program staff are responsible for securing confidential information from unintended disclosure to non-HIV/STD/TB staff. Submit all documents (annual security and confidentiality training certificates and TB/HIV/STD Confidentiality Agreement) to the Section Privacy Coordinator.

Overall Responsible Party (ORP): DSHS official who accepts overall responsibility for implementing and enforcing HIV, STD, and TB 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 HIV/STD Section Director is designated as the Overall Responsible Party. The ORP is also responsible for ongoing review of security standards as technology changes. Agencies receiving direct funding from CDC may have their own ORP in addition to the DSHS ORP.

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): An individual's health information 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, 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 Privacy Coordinator, 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 includes 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 Privacy Coordinator: The HIV/STD Section Privacy Coordinator represents the Overall Responsible Party (ORP) in enforcing 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 Privacy Coordinator serves as a resource to the LRPs.

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

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

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

III. 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. You can find the current version of the LRP handbook on the **DSHS HIV/STD website**.

The LRP Handbook provides a guidance for LRP(s) to ensure HIV/STD and TB security policies and procedures are implemented and enforced to protect confidential information within their organization. DSHS 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).

The DSHS 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 HIV/STD Section Privacy Coordinator at DSHS.

IV. Local Responsible Party (LRP) Responsibilities

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

The LRP and/or their designee will ensure staff complete security and confidentiality training, assure proper documentation is submitted for each staff to activate or maintain security access, maintain copies of staff security documents, complete and submit bi-annual reports, 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:

1. Maintain a list of all personnel authorized to access confidential information.
2. Maintain copies of current confidentiality forms and training certificates.
3. Inform DSHS when an Authorized User's access requires termination (voluntarily or non-voluntary).
4. Ensure employees complete DSHS Security and Confidentiality training annually.
5. Ensure employees submit a signed Confidentiality Agreement annually (submit with training certificate to the HIV/STD Section Privacy Coordinator).
6. Send Bi-Annual Reports and AU list to HIV/STD Section Privacy Coordinator (or Health Communications Manager if the Privacy Coordinator 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. Limit or restrict access to confidential information for any individual(s) potentially implicated in a privacy incident until the privacy incident investigation is complete.
9. Consult with the HIV/STD Section Privacy Coordinator about privacy incidents, as needed.
10. Establish and/or enforce corrective or disciplinary actions in conjunction with agency management, as needed.
11. Ensure organizational policies align with DSHS HIV/STD security policies.
12. Validate agency AU access requests for DSHS databases.

NOTE: Non-HIV, STD, or TB staff who perform duties with HIV, STD, or TB information must meet the same documentation and training requirements as an Authorized User. While any staff may take the DSHS Data Security and Confidentiality training, only staff requiring access to HIV, STD, or TB data will 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 Privacy Coordinator**.

You can find instructions for requesting access to DSHS data systems, terminating user access to DSHS databases, and the process for submitting annual security renewals on the **DSHS HIV/STD Security and Database Account Management page**.

V. LRP Reporting

LRP Report: The **DSHS TB/HIV/STD Bi-Annual Security Assessment (LRP Report)** provides DSHS with an overview of agency security practices. It also supports LRPs with many security protocols within their agency. LRPs must complete and submit the LRP Report twice per year. Report coverage dates and due dates are listed in the table below.

Bi-Annual Security Assessment Submission Schedule

Period	Coverage	Due Date	Documents to submit
1	July 1– December 31	January 31	LRP Report Authorized User List
2	January 1– June 30	July 31	LRP Report

The LRP Report is based on 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).

LRP Bi-Annual Security Assessment Instructions

LRP Report

VI. LRP Change Process

A. An LRP who is relinquishing the position should notify the DSHS Section Privacy Coordinator 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 the LRP roles and responsibilities were discussed with the new LRP. The new LRP and the HIV, STD, or TB program-level director or higher responsible agency official should be copied/included in this correspondence to the Section Privacy Coordinator.

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

NOTE: Send LRP change questions to the **Section Privacy Coordinator**.

VII. Security Culture

DSHS expects all employees and contractors to develop a constructive and collaborative security culture. Aside from the laws in place dictating security practice, we need to remember we are protecting someone's private life. To simplify security practices, we 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.

A. 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:

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

B. Privacy Incident Defined

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.

Intentional: An act done by intention or design.

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

C. 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).

VIII. 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 HIV/STD section. The LRP serves as the resource to their employees and the HIV/STD Section Privacy Coordinator 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 Privacy Coordinator. If policies are unclear to you, they may be unclear to others in your agency.

A. 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 bi-annual LRP reports, and conduct inspections of your agency facilities. The LRP reporting process exists 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 Privacy Coordinator can provide an additional pair of eyes, which provides the opportunity to recognize items you may have missed.

B. Agency Policy vs. HIV/STD 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 HIV/STD Section security policies.

DSHS HIV/STD Security Policies and Procedures

Laws, Rules, and Authorizations

IX. Privacy Incident(s) and Investigations

Privacy incidents will 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. 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. **However, DSHS reserves the right to remove a non-DSHS employee's access to DSHS-owned applications as a result of privacy incident(s).**

A. 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 HIV/STD Section Privacy Incident Report form**. **Do not include PHI/PII in the report.**

B. Privacy Incident Defined

Refer to Section VII.

C. Types of Data Compromised

1. **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).

2. **Pseudo-anonymized Data:** Individual record-level data 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.

3. **Aggregate Data:** Individual-level information 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.

D. DSHS Types of Privacy Incidents

Refer to Section VII.

E. Unauthorized Incidents

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

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

F. **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 Privacy Coordinator will need to follow up with the agency's LRP to obtain these details.

G. **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.

H. **Confidential Information Compromised:** Description of the information potentially compromised. (i.e., a file of patients with names, addresses, etc.).

I. **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.

J. **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.

What happens when a Privacy Incident Investigation Occurs?

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 (in Section VII). The questions on the **HIV/STD/TB Section Privacy Incident Report 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 Privacy Coordinator.

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.

   Simple Incident Example: *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 Privacy Coordinator may inform the DSHS Overall Responsible Party. If clarifying information is needed, the Section Policy Coordinator will ask. The emphasis is a team effort to resolve the situation.

   Complex Incident Example 1: *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.*

   Complex Incident Example 2: *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 Privacy Coordinator 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.

K. Reporting Privacy Incidents

1. Immediately report privacy incidents to upper management and/or LRP.

2. Complete the **HIV/STD/TB Section Privacy Incident Report Form** (within 24 hours of discovery). The Section Privacy Coordinator will follow-up, if needed.

L. Section Privacy Coordinator Procedures

1. HIV/STD Section Privacy Coordinator will follow-up, if needed.

2. Report to DSHS Privacy Office: The DSHS Privacy Office may issue corrective action steps, including:
   - 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 Privacy Coordinator will report to DSHS Privacy Officer immediately
- **DSHS External:** Section Privacy Coordinator 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 Privacy Coordinator within an allotted time frame.

For more information, contact the **Section Privacy Coordinator**.

Breach of Confidentiality Response Policy

HIV/STD/TB Section Privacy Incident Report Form

X. 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 DSHS 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

DSHS. 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.

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.

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 outlined below:

1. The Security Team will notify (by phone and/or email) the agency of a planned on-site inspection.

2. The Security Team will 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). *These documents must be received at least 30 days, if applicable, prior to visit by the Section Privacy Coordinator/Team.*

3. The Security Team will review agency documentation.

4. The Security Team will provide a copy of the site's assessment to the organization following the inspection within fourteen (14) calendar days.

XI. HIPAA vs. CDC

A. **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.

B. Determination of Covered Entity Based on Three Rules:

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 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.

XII. 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

XIII. DSHS Secure Network Systems and Confidential Information Access

Users requiring access to DSHS data systems and/or applications must submit a request as described on the **DSHS TB/HIV/STD Security and**

Database Account Management page.

XIV. Authorized User(s) Maintenance

The LRP and/or designee must maintain a list of authorized users. Due to the large numbers of personnel who have access to confidential statewide records, LRPs must document users in a uniform manner. DSHS provides a template **Authorized User Spreadsheet** for your use. Email this spreadsheet to the **Section Privacy Coordinator** by the end of the year (due on January 31, annually). The list of authorized users is subject to random auditing.

XV. Security and Confidentiality Training

Security and Confidentiality training explains the laws, rules, and guidelines individuals must follow to comply with DSHS HIV/STD Section security policies. Initial security and continentality training is required for each staff requiring access to confidential HIV, STD, or TB 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 initial training, staff must take the Security and Confidentiality training annually. This requirement includes employees (permanent and temporary), IT staff, volunteers, students, and contractors. See the **DSHS TB/HIV/STD Security and Database Account Management page** for instructions to take the online course and submit verification.

Train the Trainer: Agencies may wish to provide the security and confidentiality training requirement in-person and/or develop an agency owned online training module (which will cover, at a minimum, DSHS required curricula). The agency can request a training package from the **Section Privacy Coordinator** at least one-month prior to training.

Requirements for Train the Trainer:

A. Follow to all required forms and requirements. At a minimum, DSHS required curricula must be included.

B. Provide documentation of individuals who completed trainings (i.e., sign-in sheets and/or certificate of completion, and a spreadsheet with last Name, First Name, Agency email, Site, Agency Address, and agency zip code.)

Data Security and Confidentiality Request

Send required documentation to the **Section Privacy Coordinator** within 30 days of completed training (for large group of trainees). If more time is needed, contact the Section Privacy Coordinator.

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

XVI. Provisional Policies

DSHS HIV/STD security policies cannot cover every situation, technology, or workflow. To address these emerging matters, DSHS created an LRP protocol to assess any new workflow, technology, or methodology not covered by existing DSHS HIV/STD Section security policy and/or procedure. New practices must be reviewed and approved by the **Section Privacy Coordinator** prior to implementation. Submit the following information:

- 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 a new practice may be contingent upon provisions set by the Section Privacy Coordinator. The use of a new practice without prior approval will be in violation of security policies and will be treated accordingly. Consult the **Section Privacy Coordinator** if you have any questions.

XVII. Community Based Organizations (CBO)

Community Based Organizations that do not contract with DSHS must 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 Privacy Coordinator and inform of your status. DSHS requires CBOs to:

A. Establish an LRP to serve as a point of contact for privacy incidents and investigating privacy incidents. See Section IV for LRP responsibilities.

B. Assure staff complete Security and Confidentiality training annually. File documentation with the **Section Privacy Coordinator** within seven (7) days of completion.

C. Assure staff complete and sign a Confidentiality Agreement annually. File documentation with the **Section Privacy Coordinator** within seven (7) days of completion.

D. Maintain a spreadsheet of Authorized Users. Refer to Section XIV.

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

DSHS HIV/STD Section

dshs.texas.gov/hivstd