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

2016.01

TB/HIV/STD Section Confidential Information Security Procedures

Procedure Number	2016.01
Effective Date	August 1, 2016
Revision Date	July 17, 2017
Subject Matter Expert	TB/HIV/STD Section Security Officer
Approval Authority	TB/HIV/STD Section Director
Signed by	*Greg Beets*

1.0 Purpose

This document establishes general procedures that all TB/HIV/STD staff, located in the DSHS Central Office, regional, and contracted sites must follow when collecting, transmitting, storing, and maintaining confidential information in the office and in the field.

2.0 Responsibilities

Confidential information handled in the course of work activity must not be divulged to unauthorized persons in any manner that may be construed to link an individual with a communicable disease. All staff are expected to handle each situation in a professional manner that safeguards the privacy of individuals.

3.0 Definitions

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

Authorized Access: Permission granted to an authorized individual to see confidential or potentially identifiable public health data by the Overall Responsible Party (ORP)/Local Responsible Party (LRP) or designee based on the public health role of the individual and his/her need to know.

Authorized Users: Individuals who have completed the THS Section security training, have a valid confidentiality agreement on file, and have been granted access to confidential information to carry out their assigned duties.

Central Office: The TB/HIV/STD Section (THS) and its Branches, located at the Department of State Health Services (DSHS) main office in Austin, Texas.

Confidential Information: Any private information about an identifiable person who has not given consent to make that information public.

Confidentiality: The ethical principles and/or legal requirements to prevent unauthorized disclosure of any confidential information relating to patients, clients, and/or research participants.

Electronic Health Record: The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. EHRs may contain patient demographics, progress notes, problems, and medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports.

Encryption: The manipulation or encoding of information so that only parties intended to view the information can do so. As of 2015, the most commonly available systems involve public key and symmetric key cryptography.

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

Global Positioning Device (GPS): Typically a hand-held or vehicle-mounted navigational system using Global Positioning System (GPS) technology to triangulate any given position using satellite signals.

Key Card: A badge containing magnetically coded information that unlocks doors when placed in the proximity of a reading device. Key cards are used as part of physical security systems. Key cards are sometimes also referred to as name badges.

Local Responsible Party (LRP): An official who accepts responsibility for implementing and enforcing Section policies and procedures related to the security and confidentiality of TB/HIV/STD surveillance, epidemiology, public health follow-up, and medication program data and information for a specifically defined workgroup. The LRP is responsible for reporting and assisting in the investigative breach process. LRPs will be designated both internally and externally.

Mobile Device: Any portable device that is capable of receiving and/or transmitting data. Devices include, but are not limited to: laptop and notebook computers, handheld computers, pagers, tablets, and digital/cellular telephones.

Overall Responsible Party (ORP): The DSHS official who accepts overall statewide responsibility for implementing and enforcing TB/HIVSTD and Viral Hepatitis security standards and practices. The ORP is responsible for protecting data as they are collected, stored, analyzed, and released. Annually, the ORP must also provide certification to CDC that all program security requirements are being met. The THS Section Director is the designated ORP in Texas.

Password-Protected: Files and directories that are protected from unauthorized access by requiring users to enter a password before access is allowed.

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

Public Health Purpose or Public Health Data Use: Population- or individual-based activity aimed primarily at the prevention of injury, disease, or premature mortality. This term also refers to the promotion of health in the community, including 1) assessing the health needs and status of the community through public health surveillance and epidemiological research; 2) developing public health policy; and 3) responding to public health needs and emergencies. Public health purposes can include analysis and evaluation of conditions of public health importance and evaluation of public health programs.

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

Secured Area: A confined physical space housing TB/HIV/STD data and information with entry limited to staff with authorized access. Secured areas are usually defined by hard, floor-to-ceiling walls with locking doors and may include additional measures (e.g., alarms, security personnel).

A secure area must be protected by at least one level of physical security, although it is preferable that TB/HIV/STD information be maintained behind two levels of physical security. Examples of physical security levels are:

- Secured access card reader access
- Locked door
- Reader Code Access

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

Secured Drive: A drive that restricts access to information stored on the drive by anyone who is not authorized to view it, i.e. by the use of encryption and/or network mapping.

Secure Voicemail: A password-protected voicemail system that stores messages on a protected network. The requirement for individuals to enter codes to access their voice messages should not be interpreted as a secure voicemail system. These systems usually have people with administrative access that can access the messages without your knowledge or consent. Consult with your telecom administrators to identify the security level of your voicemail system.

Surveillance: The ongoing and systematic collection, analysis, and interpretation of health data to describe and monitor a health event. Surveillance information is used to assess public health status, trigger public health action, define public health priorities, and evaluate programs.

THS Section: The TB/HIV/STD Section, which includes the HIV/STD Prevention and Care Branch, the TB/HIV/STD Epidemiology and Surveillance Branch, the TB and Refugee Health Services Branch, and the Pharmacy Branch.

Treatment: The provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another

Wi-Fi (Wireless Fidelity): Equipment and systems that use high-frequency radio waves rather than wires to communicate. Wi-Fi is commonly used to wirelessly access the internet or a local network.

Wiki: A piece of server software that allows users to freely create and edit web page content using any web browser; Wiki supports hyperlinks and has simple text syntax for creating new pages and cross links between internal pages.

4.0 Physical Security

4.1 Buildings/Offices

1. All confidential information, electronic and paper, must be maintained in a secure locked area with limited access.
2. The Local Responsible Party (LRP) for each site is responsible for maintaining the physical security levels of the site.
3. The LRP for each site is responsible for maintaining a log which identifies all individuals with access to secured areas.
4. Rooms containing confidential information must not have windows that could allow easy entry into the room or easy viewing of the information from outside.
5. Keys, key cards, and codes enabling access to secure areas as defined above must not be shared or loaned.
6. All secured areas that allow visitors must have a process for tracking visitors' access.
    - Visitors to secured areas must be escorted at all times.
    - Persons with authorized access to secure areas must have a visible way to identify visitors (e.g., visitor identification badge).
    - Employees' family members are not allowed in work areas where confidential information is processed/handled.
7. Secured doors cannot be propped open or disabled without prior approval from the LRP.

4.1.1 The following apply **only** to DSHS TB/HIV/STD Section and Branch employees:

1. Internal hallways doors will be kept closed at all times
2. HHSC issues the key card/name badge to each new employee that gives the employee access to the DSHS main campus buildings. The employee presents the key card/name badge to the appropriate Branch Staff Services Officer to give an employee access to building 636. All employees are required to wear their key card/name badge clearly and visibly at all times during business hours. Employees should question anyone in the building who is not wearing a key card/name badge.

4.2 Computer Workstations

1. Computer workstations with access to confidential information must be located in a secure area. A secure area must provide at least one level of physical security, although it is preferable that workstations with access to TB/HIV/STD information be kept behind two levels of physical security.
2. Computer screens that display confidential information must not be readily observable by non-authorized users in the office area. Security screens may be installed on computer monitors to prevent viewing of information by anyone other than the operator.
3. Computers that access confidential information must be password-protected at the Windows login level; a password-protected screensaver program must be installed that activates after a few minutes of inactivity by the user.
4. All network/computer passwords are to be at least eight characters long and must be a combination of letters, characters, and numbers.
5. Network/computer passwords must expire based on current password guidelines.
6. Temporary passwords must expire once the user generates a password.
7. Users must never share their passwords.
8. No one should access a computer or network using another person's access without prior written authorization in specific situations (e.g., MMP data collection staff cannot obtain individual access to a patient's medical record at a participating MMP medical facility).
9. When a password's security is in doubt, change it immediately.
10. Passwords should not be written down.
11. Computer workstations must be locked (Ctrl/Alt/Delete - Lock Workstation) whenever a workstation is unattended.
12. Internet Control Message Protocol (ICMP) should not allow "Redirect Services" to devices (e.g., smartphones, tablets) not authorized by network administrators.
13. Network services should not allow "remote desktop" access by non-network users.
14. Local hosting of servers (e.g., "Wikis") on computers that access confidential information is a security risk and should be avoided whenever possible.
15. Confidential data must not be accessed on any computer that is not secure.
16. Computers at external locations with access to DSHS systems and/or networks must conform to DSHS Information and Security standards.

5.0 Handling Paper Records

5.1 In the Office

1. Confidential information must be kept in a locked file cabinet in a locked secure area when not in use.
2. Confidential information must be returned to secure storage immediately after use.
3. Texas HIV Medication Program (THMP) applications and supporting documents may not be removed from the THMP office.
4. Confidential information must not be readily observable by non-authorized users as they pass through the office, sit at desks, or approach reception areas.
5. Confidential information must be maintained and destroyed according to the DSHS/HHSC records retention policies and/or local records retention policies.
6. Confidential documents must be shredded before disposal using a commercial-grade shredder with a crosscutting feature.
7. Shredding of confidential documents must be conducted by persons authorized to view the confidential information. If shredding is outsourced, the shredding must be done on site in the presence of a staff member. All shredding or disposal contractors must be bonded.
8. Confidential documents to be shredded must be stored in a secure area.
9. Stored confidential documents must be clearly marked as containing confidential information. Containers must not be labeled as having TB, HIV, or STD documents.
10. A supervisor or LRP must pre-approve any situation (e.g., business travel) when confidential information cannot be returned to the secured area by the close of business on the same day.
11. Confidential documents must not be readily observable by non-authorized users as they pass through the office, sit at desks, or approach reception areas.
12. Copies of a Field Record will not be made for any unauthorized purpose.
13. Removing Interview Records from the workplace is prohibited.
14. Interview Records must not be destroyed, except as directed by the supervisor and in the manner described for the Field Record.
15. The existence of, or contents contained in, an Interview Record will not be divulged to any unauthorized persons.
16. For TB/HIV/STD central office programs all paper needs to be placed in the locked recycling bins for shredding and not in any other recycling bin.

5.2 Outside the Office

1. Workers should only remove confidential information from a secured area for immediate use.
2. Confidential documents must not be left unattended in any place where unauthorized persons may gain access. If confidential information is suspected lost or stolen, notify the supervisor and the LRP immediately.
3. Confidential documents (e.g., Field Records, TB case documents) must not be taken to a private residence, place of business, or other location other than a client residence (and only those documents relevant to the client) or the staff person's vehicle. A supervisor or LRP must pre-approve unavoidable situations (e.g., PHFU activities conducted during non-business hours) where a staff person has to bring confidential documents to his/her residence.
4. Confidential documents (e.g., Field Records, test results to be provided to a client) taken to the field must:
    - be kept in a secured locking briefcase,
    - contain only the minimum amount of confidential information necessary to do business, and,
    - be coded to disguise any information that could easily be associated with TB/HIV/STD, where possible.
5. If confidential information is taken into the field, it must be carried in a manner that insures against loss or inadvertent display. Field Records will be properly coded and code sheets will not be carried in the field.

6.0 Telephone, Faxing and E-mail

6.1 Telephone (including cell phones)

1. Telephone calls concerning confidential information must be made in an area where conversations cannot be overheard. Calls conducted from a staff person's home must be conducted in a private room, where conversations can't be overheard.
2. Staff must reasonably ascertain that phone contacts are legitimate before discussing confidential information on the phone. Sharing specific information about individuals with an authorized person will be done according to local policies and only after taking the reasonable precautions to confirm the identity of the authorized person (e.g., asking for two forms of identification).
3. Staff will only share the minimum amount of confidential information needed to accomplish the business objective of the call. For the Medical Monitoring Project (MMP) purposes, MMP staff should not use the words "HIV" or "AIDS" when

speaking to a patient by phone. If necessary, it is only allowed after the patient's identity has been verified by two forms of identification (i.e. date of birth, their address, etc.) and only if the patient uses the words HIV or AIDS first.

4. When conducting a MMP telephone interview (TI), it is necessary to first confirm the patient's identity by requesting two forms of identification such as date of birth, their address, and/or patient's provider name before beginning the TI or mentioning HIV or AIDS.
5. Confidential information must not be left on voicemail systems unless staff have verified that the system is secure (cell phone voicemail systems are generally not secure) or there is written authorization from the call recipient to leave confidential information.
6. Outgoing voicemail messages on telephones with non-secure voicemail must ask the caller to leave only their name and number.
7. Outgoing voicemail messages must not identify staff as being employed by the TB/HIV/STD Section or its Branches.
8. If an employee on a confidential call hears other conversations on the line ("cross talk") or similar issues, the call must be ended immediately and reported to the LRP.
9. Lab results may be furnished to clients over the telephone in accordance with local policies and safeguards. This includes notifying clients of a negative HIV test result. Positive HIV test results must not be given by telephone.
10. If someone calls on an applicant or program recipient's behalf, staff must reasonably ascertain that the contact is legitimate before discussing any confidential information. Legitimate contacts include the applicant or recipient's doctor, pharmacy, or case manager. Confidential information may also be released if there is written authorization for the release.
11. If in doubt, ask the caller if the person s/he is calling about is available to speak on the phone in order to confirm his/her identity and provide verbal consent to speak to the caller on his/her behalf.

6.2 Faxing

1. Fax transmission of confidential information must only be done when other transmission methods are unavailable or would delay the timely provision of the service.
2. Confidential information sent via fax must be under a cover sheet. The cover sheet cannot contain the words TB, HIV, AIDS, or STD.
3. The electronic HIV/AIDS Reporting System (eHARS) city no., state no., and unique identifier (UID) are considered identifying variables and should not be included in faxes.
4. Faxed confidential information must be de-identified (client's name and all other identifying information removed).
    - If this is not possible, identifying information must be sent in a separate fax transmission only after the sender has confirmed receipt of the first fax

    OR

    - All TB/HIV/STD-related information must be removed or converted to code.
5. Anyone faxing confidential information must confirm the information was received by the intended recipient.
6. Fax machines used to send or receive confidential information must be located in a secure area.
7. If possible, programs should use separate fax machines instead of multifunctional machines with faxing capabilities.
8. The following procedures apply to THMP records:
    - Outgoing order faxes will only be sent to the pharmacy fax number listed in the HIV2000 database.
    - THMP information should only be faxed directly to the client, case manager, clinic, doctor's office, or pharmacy.

6.3 E-Mail

1. Email, encrypted or non-encrypted, must not be used to transmit confidential information except those that meet the DSHS-specific treatment exception (6.3.6). Emailing attachments containing confidential information is also prohibited. The eHARS city no., state no., and UID are considered identifying variables and should not be included in emails or attachments.
2. Email and confidential information must not be accessed simultaneously to avoid accidental transmission. This includes any electronic device with internet capabilities.
3. MMP staff must include a signature in the email body stating, "Please do not reply to this email with any patient identifying information. This includes: name, phone number, DOB, address, and medical record numbers. Please call me on my private line at (###) ###-#### with this information."
4. Do not use "HIV," "AIDS," or "STD" in email signatures.
5. When emailing the CDC, Data Coordinating Center (DCC) or Cerner, do not include the MMP patient identification number (PID) or facility identification number (FacID). These are considered Personal Health Information (PHI) according to the federal security standards.
6. Treatment Exception (*Applies only to DSHS*): Emails being used for the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another may be sent using DSHS agency email.

Any PHI must be in a file that is encrypted and attached to the email, not in the body of the email itself. The DSHS agency email policy for sharing confidential PHI must be followed, it states.

- Confidential DSHS information and an individual's full name, or first initial and last name along with restricted personal information, such as social security number, government-issued identification number, driver's license number or Medicaid number and PHI transmitted over network connections must be encrypted using the 'Send Secure' email function or otherwise protected as required by rule or law and agency policy and procedures. Do not include confidential information in the subject line of the email since the subject line is not encrypted.

7.0 Handling Confidential Mail

7.1 Incoming Mail

1. All mail marked "confidential" or ATTN (mail code) MSJA, must be checked by only authorized personnel and kept in a secured location until it is processed.
2. Mail marked "confidential" should only be opened by the addressee.
3. The person in charge of receiving confidential mail must notify the sender on the day of receipt.

7.2 Outgoing Mail

1. Confidential information sent through the mail must be double-enveloped.
2. Confidential information must first be placed in a sealed, taped, non-addressed envelope marked "CONFIDENTIAL." That envelope is then placed in a second sealed-and-taped envelope marked "CONFIDENTIAL" and "TO BE OPENED BY ADDRESSEE ONLY."
3. The outer envelope must contain the return address of the sender. The words "TB," "HIV," "AIDS," and/or "STD" must not appear in the body of the address or return address. This also applies to address stamps and/or pre-addressed envelopes.
4. Program correspondence to applicants, program enrollees, service providers, and pharmacies will be sent in a security-tinted envelope to the mailing address listed in the program database.
5. If a program enrollee indicates s/he does not want mail sent to him/her, this should be indicated in the program database.

8.0 Handling Electronic Data

NOTE: *The Section recognizes that as technology continues to evolve, so also may the HHSC IT Security Guidelines and the CDC federal standards. In all cases, the requirements to be met must be the most restrictive of the two.*

8.1 Electronic Data Access

1. Network drives, which contain confidential information, must have controls in place that prevent unauthorized user access.
2. Staff must not attempt to access any data, program, or system without approved authorization. Access to THMP program databases will only be granted to THMP staff, approved contractors, and appropriate application development and support staff.
3. In the case of remote access from approved home-based computing devices, firewall, anti-adware/spyware, and anti-virus protection, appropriate security patch levels must be installed, active, and maintained by the remote user.
4. Non-DSHS systems that require network connectivity must conform to DSHS standards/policies and must be approved by DSHS IT Security.

8.1.1 The following apply **only** to DSHS TB/HIV/STD Section and Branch employees:

1. The Branch/Group Manager(s) has the responsibility to ensure that departing employees' access to program databases is terminated after they leave employment and to remove the key card/name badge from the building security system. In addition, Branch/Group managers will routinely request building access reports to review the level of access by current staff and that former employees have been removed from the building security system.

8.2 Electronic Data Storage

1. Electronic data must be held in a technologically secure environment; the number of data repositories and the number of permitted users must be kept to a minimum.
2. Personal computers or personal electronic media should not be used for data storage. Data Storage devices must be issued by the agency. Only an agency-issued device, internet service provider (ISP), or personal network equipment may be used for internet connectivity.
3. Confidential information must either be stored on a computer which is not connected to a network (i.e., stand-alone computer) or on a secure drive of a secure network (e.g., network with restricted access and/or firewall protection). An

agency must have properly configured firewalls installed on computers to be used outside of the agency's secure network.

4. Confidential information should never be stored on the hard drive of any computer connected to a local or wide area network (WAN). PHI should never be stored on a device that is connected to the internet, either directly or indirectly, outside the agency firewall.
5. Agency issued computers must be configured to prevent installation of software by persons other than agency IT staff.
6. Stored datasets containing PHI must be encrypted using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES) **FIPS-197** (PDF) [U.S. National Institute of Standards and Technology] and stored either on a stand-alone computer or on a secure drive. (Data at Rest standard)
7. Confidential data should not be stored on wireless handheld devices. In the event there is no alternative to local storage, all sensitive, confidential, and restricted personal information, including PHI, must be encrypted.
8. MMP information stored on Google Drive must not contain any patient identifying or confidential information. No other program information shall be stored on Google Drive or other cloud storage providers.

8.3 Electronic Data Transmission

1. Confidential electronic information transferred between the Central Office and external sites, and between external sites, must be encrypted and transferred using secure networks approved by the LRP. File encryption must be done prior to uploading to the secure network using software that meets federal AES standards. Winzip is an example of an approved encryption software and is recommended.
2. Any system used to electronically transfer data must receive prior approval from the ORP. Such systems must include access controls and encrypt all identifiable data prior to transfer.
3. Confidential information transmitted electronically between Central Office and external sites, and between external sites, must be sent over the Texas Public Health Information Network (PHIN). PHIN user instructions are located at **www.txphin.org**.
4. All employees, providers, and vendors are prohibited from using or installing any device which functions in wireless mode in order to access data, transfer data, or connect in any manner to DSHS networks or systems without the approval of the DSHS IT security and assistance from DSHS IT.
5. Bluetooth is an open standard for short-range radio frequency (RF) communication. When deploying Bluetooth for business devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets, sites must use the strongest Bluetooth security mode available for their devices.
6. The default settings on Bluetooth-enabling devices must be reviewed and changed as needed so that they comply with all applicable security policy requirements. All unneeded Bluetooth profiles and services must be disabled to reduce the number of vulnerabilities that attackers could attempt to exploit. Users must be provided with a list of precautionary measures or additional security awareness training so they are fully informed of Bluetooth-related security risks and protecting handheld or wireless devices from theft.
7. VPN access to DSHS networks must be controlled via password authentication, token devices, or public/private key systems incorporating a strong pass-phrase.
8. Any computing device connected to DSHS networks or other technology must be protected by the use of a firewall that meets DSHS standards.
9. Any computing device connected to DSHS networks or other technology must use anti-virus software and configurations approved by DSHS IT. Configuration must include real-time, as well as passive scanning, and maintain current virus definitions.
10. VPN connections will be automatically disconnected after a period of non-use or inactivity. In this event, the User must log in again. Use of any technology to maintain an inactive connection (ping, stay-connect, etc.) is prohibited and can result in termination of the VPN account.
11. Users of any computing device not owned by DSHS must configure that device to comply with all DSHS standards and security policies while connected to the DSHS networks.
12. The use of any VPN client, other than the one provided by DSHS or its service provider, is prohibited when connecting to a DSHS application.
13. All MMP interview data must be transmitted to the CDC using the Data Coordinating Center (DCC) which is administered by ICF Macro.
    The DCC data portal:
    - is a secure, web-based system that uses secure socket layers (SSL) technology,
    - is protected by the most secure certification process available (green address bar),
    - can be accessed from any web connection,
    - uses login/password security for access to the system that can be accessed at **www.dcc-dataportal.org**, and
    - assigns users a specific level of system access, depending on their MMP role.
14. All MMP medical chart data must be collected on an internet web browser called Discovere® administered by Cerner. The Discovere® URL is **https://discoverecdc.cerner.com**.

- Discovere® requires each system user to have a unique user ID (also referred to as a user name) and a private password. You must enter your user ID and password each time you access Discovere®.
- Discovere® is compatible with all major web browsers, but is currently certified for use with Internet Explorer 8, 9, 10, Google Chrome, and Mozilla Firefox. If you are using Internet Explorer, there are some custom settings that must be in place to optimize the Discovere® experience.

15. Confidential information transmitted electronically between Central Office and the CDC must be sent over the Secure Access Management Services (SAMS) according to instructions provided by the CDC.
16. All confidential information transmitted electronically between the THMP, Medicare, Medicaid, or contractors must be encrypted and password-protected. Data should be transferred using a secure FTP server or the File Transfer Utility built into the HIV2000 system.

9.0 Mobile Devices

All staff are individually responsible for protecting any assigned or personally owned portable device used to access confidential information. Affected devices include, but are not limited to: laptops, smartphones, cell phones, flash drives, diskettes, CD-ROMS, zip disks, tape backups, removable hard drives, smart cards, and/or GPS systems.

All staff must follow Section 1.9 Electronic File Transfers, 1.23 Portable/Remote Computing, 1.25 Removable Media and 1.33 Wireless Computing of the **Texas DSHS Information Security Standards and Guidelines** (only accessible to computers on the DSHS network). If there are differences between the DSHS Information Security Standards and Guidelines and standards stated in this document, the stricter of the two applies.

9.1 Laptops/Netbooks/Tablets

1. Confidential information may not be stored on the hard drive of a laptop computer. All confidential information must be encrypted with encryption software that meets FIPS-197 AES requirements and is stored on a removable storage device. The removable storage device must be separated from the laptop and stored in a secure location when not in use.
2. The media on the device being used to access confidential information must be fully encrypted; encryption of individual files is not adequate. Laptop hard drives must be encrypted.
3. When working with confidential information on a laptop computer, staff must ensure that unauthorized users cannot view the screen.
4. Laptops used in the workplace fall under the same confidentiality and security guidelines as workstations (see physical security section).
5. Laptops must not be left unattended in non-secure areas. Unattended laptops should either be stored in a locked room or a locked file cabinet.
6. When traveling with a laptop, use a lockable carrying case. If you do not have one, a form-fitting padded sleeve for the laptop carried in a backpack, courier bag, briefcase, or other common nondescript carrying case may be used, if approved by the LRP.
7. When transporting a laptop, it is safer to rent or use a car with a locking trunk (not a hatchback/minivan/SUV). Regardless of vehicle type, laptops must never be visible from outside of the car.
8. Portable computers with wireless connectivity capabilities (built-in or attached) must follow appropriate DSHS Information Security standards when working with confidential information. Staff must not use any laptop containing confidential information to access the internet via hotel or other non-secure public access networks.

9.2 Removable Storage Devices

1. Only encrypted removable storage devices issued by DSHS may be used with DSHS-owned computers. Use of non-DSHS-issued removable storage devices is prohibited.
2. All confidential information placed on a removable storage device must be password-protected and encrypted using encryption software that meets FIPS-197 AES requirements. The password must be stored separately from the device. Affected devices include, but are not limited to:
   - Diskettes, tapes and/or compact discs (CDs),
   - Memory cards/sticks used in various portable digital devices,
   - Firewire/USB “Flash/Key/Pen/Thumb” drive memory devices, and
   - Portable mass storage devices (e.g., external hard drives).
3. Any removable storage device containing confidential information is to be stored following the physical and electronic standards outlined in these procedures.
4. Removable storage devices containing confidential information cannot be taken to a private residence without prior, specific permission from the LRP.
5. Removable storage devices no longer in use must be destroyed.
6. Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse. Alternately, the diskettes and other storage devices may be

physically destroyed (e.g., by incineration, shredding); physical destruction should include the device, not just the plastic case around the device.

7. If a removable media device containing confidential information is being mailed to another location, the device must be:
    - labeled as confidential with a return address,
    - physically handed off and signed for, and
    - tracked until it reaches its final destination.

9.3 Smartphones/Cell Phones

1. Users of smartphones, cell phones or any equivalent system must follow all electronic media and physical storage standards listed in these procedures.
2. Confidential information must not be stored on or accessed from a smartphone, cell phone, or any equivalent system.
3. The capturing, storing, and/or transmitting of any image (still or in motion) is prohibited while in secure locations housing confidential information or when interacting with clients. Staff must disable any image-capturing function on smartphones, cell phones, or related devices while in secure locations or when interacting with clients.
4. Confidential phone calls should not be used with Bluetooth unless traveling alone in a Bluetooth- enabled vehicle so the driver can safely speak hands-free.

9.4 GPS Systems

1. Staff are responsible for ensuring that their GPS systems are secured from damage and/or theft.
2. Staff are responsible for ensuring that address information entered into these systems cannot be linked in any way with a TB, HIV, or STD client.

9.5 Lost or Stolen Devices

1. Any device that may contain confidential information that is believed to be missing or stolen will be immediately reported to their supervisor and the LRP and handled as a possible privacy incident. The TB/HIV/STD breach reporting form (**form #303.002**) needs to be completed. The breach reporting procedures in the TB/HIV/STD Section Breach of Confidentiality Response Policy (**2011.04**) must be followed.
2. All non-DSHS entities should follow their internal policies for reporting Missing, Damaged, and/or Stolen devices. It is expected these policies will include at a minimum:
    - Notify manager of area where the device has been assigned to.
    - Notify IT so device can be remotely wiped (when possible).
    - If presumed stolen, file a police report.
3. All DSHS offices should, at a minimum, follow these procedures:
    - Notify the supervisor and staff person who is responsible for assigning devices to staff (if applicable).
    - Notify IT so device can be remotely wiped (when possible).
    - If presumed stolen, file a police report.
    - Complete Form DSHS-AM02 in conjunction with supervisor.

9.6 Texting

The standards established by the Texas Health and Human Services Commission (HHSC) Text Message Policy, (#HHSC- OPS-01) for maintaining client confidentiality must be followed in all types of communications involving any individual who may have been exposed to TB, HIV, or STD.

To ensure compliance with the Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Pub L No. 104-191), text messages sent by a health department should never include an individual's protected health information.

Text messages should never include a reference to “STD”, “HIV”, “Syphilis”, “TB”, or any other identified health condition.

The following guidelines must be followed:

1. Initial text messages sent to clients should encourage them to make contact via phone. While some clients may insist on texting only, text messages should be worded to motivate the client to call since protected health information may not be shared via text.
2. Text messaging should only be done from an encryption-protected, agency-issued device. Personal devices should not be used to send text messages for public health follow-up.
3. For retention concerns, text messages are considered as transitory information and must be deleted within 24 hours after entering information into the official system of record.
4. If an agency-issued device that is used for text messaging is lost or stolen, the employee must immediately report the loss/theft to their supervisor and the local responsible party (LRP). This must be handled as a possible breach.
5. If a client texts you information that needs to be kept (ex. address, contact information, etc.) you must update the system of record (Aries, eHARS, THISIS, TB Pam, etc.) within 24 hours and then delete the text message from the device.
6. Some appropriate uses for text messages include: appointment reminders, requests for the client to contact you, confirming date and location of an appointment/interview, etc., including a comment discouraging the client from

responding to the text message with any personal information. Always contact your supervisor or LRP if you are uncertain about how to word a text message or before responding to a text message from a client who is asking for more information.

7. Avoid getting into a texting conversation; state for the protection of client privacy you are not allowed to share confidential information via a text message.

10.0 History

Date	Action	Section
9/1/2017	Changed "TB/HIV/STD Unit" to "TB/HIV/STD Section" to reflect new program designation	-
7/17/2017	Changes to email section to allow exception for treatment at DSHS-only offices.	TSH security officer, ORP
8/1/2016	Added new section 9.6 to address texting; New sections 4.1.1 to address building security issues for DSHS Unit & Branch employees. New section 8.1.1 to address manager responsibilities when their employees are departing/separating from state employment.	THS security officer, ORP
2/1/2016	Final approval by ORP	-
12/11/2015	This is a new document which combines and replaces all security procedures (PHFU, TB Services, MMP, Epi & Surveillance, and THMP) into one document.	ORP, THS security officer, THS staff and managers.

Last updated September 8, 2017