Texas Department of State Health Services

TB/HIV/STD Section Confidentiality Agreement

Name: _____

Email (Business): _____ Phone Number: _____

Job Title: _____ Agency/Site: _____

Department Name/Program: _____

The following section must be completed if submitting for annual security renewal AND you have access to one or more DSHS-owned or managed databases/applications

Account Renewal: Place a check next to the database(s) and/or application(s) you currently use and continue to have a need for access (check all that apply):			
☐ THISIS	☐ GlobalScape	☐ eHARS	☐ Citrix STD*MIS
☐ NTIP	☐ TB GIMS	☐ EDN	☐ ITEAMS (TB Only)
☐ ARIES	☐ TB Labware		
******NOTE****** Individuals who have access to a database or application that is not selected above will result in deactivation of those accounts. Access will only be maintained for accounts in databases checked above on this form.			
Date of Security Training Renewal (Date submitted to DSHS):			
Manager/Supervisor Name:			
Manager Email:		Manager Phone:	
Local Responsible Party (LRP) Name:			
LRP Email:			

BACKGROUND INFORMATION:

The Texas Department of State Health Services (DSHS) guiding principles establish the paramount importance of patient and client confidentiality in the mission of this department. Information in reports, records, correspondence and other documents routinely dealt with by employees of the DSHS may receive its designation by statute of judicial decision. Such statutes as the Open Records Act, Medical Practice Act, and the Communicable Disease Act contain provisions which make certain information that comes to DSHS privileged and/or confidential.

As a general rule, in transactions carried out on a day-to-day basis, medical records and information taken from medical records are made privileged and

confidential by the Medical Practice Act. All communicable disease records (STD, HIV and TB) are made confidential by the Communicable Disease Act. Birth and death records are made confidential for 50 years through the provisions dealing with vital statistics in the Open Records Act and other laws. If information is "confidential" it is generally information that should be kept secret and is given only to another person who is in a position of trust. "Privileged" information protects a person who has either given or received confidential information from being revealed in a legal proceeding. Other information that contains "highly intimate or embarrassing facts about a person such that its disclosure would be highly offensive to a [reasonable] person… and is not of legitimate concern of the public or might hold a person up to the scorn or ridicule of his or her peers if made public, is made confidential by the common law doctrine of the right to privacy. [ORD-262, 1080] Statutes that govern the operation of DSHS may contain additional provisions that render information that comes into the hands of certain programs in DSHS privileged, confidential and/or private.

Note to employee: If you have questions regarding confidentiality, you should contact your immediate supervisor. The signed Employee Confidentiality Agreement will be filed in your personnel folder.

The purpose of this agreement is to help you understand your duties regarding confidential information. You will be required to reaffirm your understanding of these duties on an annual basis.

Check all that apply:

☐ I am a full time or part-time EMPLOYEE of DSHS (EXCLUDES volunteers, contractors, and other users NOT on HHS payrolls) with access to what this agreement refers to as "confidential information."

☐ I am a full time or part time:

- ☐ volunteer
- ☐ contractor
- ☐ other (describe): _____

AGREEMENT:

I Agree that:

- A patient record or any information taken from a patient record is privileged and confidential. In most instances, such information may not be released unless the person identified in the record provides written consent, or the release of information is otherwise permitted by law. A patient record is defined as: a record of the identity and diagnosis of a patient that is initiated and maintained

by, or at the direction of a physician, dentist, or someone under the direction or protocols of a physician or dentist.

- I understand that I must not release information from reports, records, correspondence, and other documents, however acquired, containing medical or other confidential information, and that I may not release such information except in a manner authorized by law, such as in a statistical form that will not reveal the identity of an individual or with the written consent of the individual involved.
- I may not release or make public, except as provided by law, individual case information including demographic data and client contacts.
- I will keep all confidential files, including portable storage devices, in a locked file cabinet when not in use.
- When I am working on a confidential file, I will “lock up” the information when I leave my workstation for lunch, meetings, or for the day. I understand that to “lock up” the information includes logging off my computer, not merely saving and closing the confidential file.
- I will keep any confidential files I work with out of the view of unauthorized persons.
- I will not discuss confidential information with people who are not authorized, and/or who do not have the need or the right to know the information.
- When I work with files that contain personal identifiers, I will log off my computer when I am not actively using the file.
- To protect confidentiality, I will not discuss the facts contained in confidential documents in a social setting.
- When transporting information that is privileged, confidential or private, I will employ appropriate security measures to ensure the material remains protected.
- I will keep information relating to the regulatory activities of the department confidential. Regulatory activities include at least the following: survey schedules, unannounced site visits, survey results, information pertaining to complaints that have been investigated, litigation information, and personnel actions.
- Where applicable, departmental policy requires that personnel have individual passwords to access confidential computer files. I will not use another person’s password nor will I disclose my own.
- I understand that my supervisor will document any violations of this agreement and he or she will place the documentation in my main personnel file maintained by Human Resources.

- If I am a professional employee (e.g., a physician, registered nurse, attorney, etc.) or I am an employee supervised by or providing support to a professional employee, I understand that I may be subject to additional rules of confidentiality. This agreement does not supersede the code of professional conduct and I further understand that a violation of the code of professional conduct may subject the professional employee to additional sanctions (e.g. loss of license).
- When I dispose of a document that contains patient information, I will assure that the document is shredded.
- I understand my obligations under this Agreement will continue after termination.
- I will report activities by any other individual or entity that I suspect may compromise the confidentiality, integrity or availability of confidential information. Reports are made in good faith about suspect activities and will be held in confidence to the extent permitted by law.
- I understand that email, encrypted or non-encrypted, must not be used to transmit confidential information except those that meet the DSHS-specific treatment exception (***exception only applicable to select DSHS employees only—see TB/HIV/STD Security policy, Section 6.3.6).
- I have read and will abide by DSHS TB/HIV/STD Policies and Procedures including the TB/HIV/STD Security Policy and any relevant or applicable policies and procedures implemented by the entity for which I am employed. I further understand that failure to adhere to DSHS and/or my direct employer's policies and procedures could result in adverse personnel action, up to and including the revocation of database access and/or termination of my employment.

I have read this confidentiality agreement and I understand its meaning. ***I further understand that should I improperly release or dispose privileged, confidential, or private information, or break any terms of this agreement, I may be subject to an adverse personnel action, up to and including the revocation of database access and/or termination of my employment.*** In addition, I understand that I may be subject to civil monetary penalties, criminal penalties or liability for money damages for such an action.

Employee's Name: _____

Employee's Signature and Date: _____

Electronic signature required
How to create a digital signature in Adobe