## Purpose

To ensure each client's information and record, whether on paper or in an electronic format, is treated with confidentiality and is kept secure in accordance with the Texas Licensing Standards for Home and Community Support Services Agencies at §558.301, per the federal standards found in the Health Insurance Portability and Accountability Act (HIPAA), and other applicable state and federal regulations.

## Policy

A. The Agency will ensure that all of the client's protected health information (PHI) and electronic protected health information (ePHI) will remain confidential and will be secured and controlled whether on paper, in an electronic format, or a combination of both in compliance with the Privacy Rule of the Administrative Simplification provisions of HIPAA, the HITECH Act of 2009, the Texas House Bill (HB) 300 of 2012, and other applicable state and federal regulations.

1. The state regulations include the Data Use Agreement (DUA) and the Security and Privacy Inquiry (SPI) that are incorporated here by reference for those contracting with Texas Health and Human Services (HHS).

## Definitions

A. Breach: an impermissible use or disclosure that compromises the security or privacy of an individual's protected health information or electronic protected health information, known collectively as protected health information.

B. Business Associate: a person or organization that performs certain functions or activities on behalf of, or provides services to, a covered entity that involve the use or disclosure of individually identifiable health information; includes the Agency's contractors and subcontractors of organizations.

C. Covered Entity: health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form.

D. Disclose: to release, transfer, provide access to, or otherwise divulge information outside the Agency.

E. Electronic Devices: include, but are not limited to, computers, laptops, tablets, smart phones, personal digital assistants (PDAs), USB flash drives, and external hard drives.

F. e-PHI: electronic protected health information is all of an individual's identifiable health information the Agency creates, receives, maintains, or transmits in electronic form.

G. Health Information Technology: includes digital tools and services such as mobile phone apps and email messaging that can be used to enhance a client's self-care, facilitate client-provider communication, inform health behaviors and decisions, prevent health complications, and promote health equity.

H. HITECH Act: Health Information Technology for Economic and Clinical Health Act expands the types of businesses covered by HIPAA, allows clients to more directly access their electronic health records, requires covered entities to notify clients of breaches, and encourages "meaningful use" to improve communication between health care providers in direct relationships for client care.

I. Meaningful Use: the use of certified electronic health record (EHR) technology in a meaningful manner and ensuring that it is connected in a manner that provides for the electronic exchange of health information to improve the quality of care.

J. Notice of Privacy Practices: the Agency's description of how the client's individually identifiable health information may be used, disclosed, and accessed.

K. Personally Identifiable Information (PII): any information about an individual maintained by the Agency including that which can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

L. Privacy Officer: provides oversight of the Agency's compliance with its policies and procedures related to the client's privacy and security of records by monitoring compliance with its policy on confidentiality and privacy of information.

M. Protected Health Information (PHI): individually identifiable information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium; but, excludes individually identifiable information in education records covered by the Family Educational Rights and Privacy Act, in employment records held by a covered entity in its role as employer, and regarding a person who has been deceased for more than 50 years.

N. Risk Analysis: an ongoing process in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures that have been put in place, and regularly reevaluates the potential risk to e-PHI.

O. Security Officer: security official who is responsible for developing and implementing the Agency's security policies and procedures.

P. Unsecured Protected Health Information: protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services (HHS).

**Procedure - Clients**

A. The Agency’s Supervisor evaluating the client for admission will verbally explain to him/her or the client’s representative that the Agency will keep all his/her records and information confidential and secure from impermissible use or access. This information will be provided at the earlier of:

1. The time the client is admitted to receive services from the Agency; or
2. The time the Agency begins providing services to the client.
3. The client or the client's representative will be given a copy of the Agency's Notice of Privacy Practices that is included here by reference.
    a. The client or the client's representative will be notified 30 days before changes are made to the Notice of Privacy Practices if the Agency changes it or if the HIPAA rules impacting it change and s/he will be given the opportunity to:
        i. Accept the policy change(s) prior to any new use or disclosure of his/her health data; or
        ii. Be allowed to terminate his/her contract or user agreement with the Agency.

4. It will be explained that sources who may have access to the client's records, without his/her consent, include other treatment providers for coordination of care, payor sources including, insurance companies or Managed Care Organizations (MCOs), regulatory agencies including Texas Health and Human Services (HHS), contracted consultants and other Business Associates, public health agencies, the Agency for limited use for marketing purposes, and as required by law.
    a. The Agency will produce copies of its policies and procedures and records relating to the use or disclosure of PHI or ePHI within three (3) business days of the request by HHS.
5. The client or the client's representative will sign and date on the Consent form acknowledging this information has been provided.
    a. The Agency's representative will sign and date the Consent form, also.
    b. If the client is unable to sign/date the Consent form, the reason why will be provided on the form.
    c. The original signed/dated Consent form will be kept in the client's record at the Agency and a copy will be given to the client or the client's representative.

B. The client or the client's representative may contact the Privacy Officer in writing to request access to the client's paper or electronic records at any time during the course of care.
1. The Agency will provide the requested information, whether on paper or electronically, within fifteen (15) days of receiving the request.
2. The client or the client's representative may request that the Agency provide the information to protect his/her privacy and confidentiality by a particular method or in a particular location other than by the Agency's usual means.
3. The written request will be placed in the client's record.

C. The client may authorize in writing for others to have access to his/her record.
1. The client may revoke this authorization in writing at any time.

D. Additional considerations for the client or the client's representative to know include, but are not limited to the following:
1. The client may request to restrict the use and disclosure of his/her PHI.
2. The client may request a copy of his/her PHI.
    a. The Agency will provide the requested information, whether on paper or electronically per the client's request, within fifteen (15) days of receiving the request.
    b. The Agency may impose reasonable, cost-based fees for the cost of copying and postage.
3. The client may request an accounting of the disclosures of his/her PHI.
    a. The Agency has 60 days to provide information on when the PHI was accessed and by whom.

b. The Agency must provide an accounting of the date, a description of the PHI disclosed, to whom it was disclosed, and the purpose for disclosures made up to six (6) years prior to the request.

4. The sale of his/her PHI is prohibited.

5. The Agency must notify him/her of a breach of unsecured PHI.

6. If the Agency conducts fundraising, the client may opt out of receiving fundraising communications from the Agency.

7. The client may restrict disclosures of PHI to a health plan with respect to health care for which the client has paid out of pocket in full.

a. The Agency has flexibility and may determine the following:

i. How to flag information that is the subject of a restriction; but, is not required to segregate the record;

ii. How the restriction requests for certain services, such as bundled services, are to be handled; and

iii. What reasonable efforts should be made to obtain payment from a client original form of payment has been dishonored, prior to resorting to billing the health plan for the service.

E. The client or the client's representative may contact the Privacy Officer and request that his/her PHI be amended or corrected.

1. The request to amend PHI can be denied if it is determined the information is accurate and complete.

a. The client or the client's representative will be notified within 60 days of the decision.

b. If the accuracy of the information is still being disputed after the denial, the client or the client's representative will be provided an opportunity to file a statement of disagreement with the Agency.

c. The Privacy Officer will document the dispute and any subsequent disclosure of the disputed PHI.

2. When corrections are made to the client's PHI, the Privacy Officer will make reasonable efforts to provide the corrected information to others who are known to have accessed that particular PHI before it was amended.

F. The client may contact the Privacy Officer if s/he has any complaints or concerns relating to the privacy and security of his/her records without fear of discrimination, coercion, reprisal, or retaliation.

**Procedure - Employees and Volunteers**

A. As part of an employee's and volunteer's orientation, s/he will be trained on the Agency's privacy policies and procedures as necessary and appropriate for him/her to carry out the assigned job functions in all of the Agency's workplaces.

1. Training will be updated as the result of changes in the Agency's policy or procedures and as a result of changes in state or federal regulations.
    a. In the event there are no changes as listed above, retraining on the Texas HB 300 will take place every two (2) years.
2. Employees and volunteers will be responsible for knowing, observing, and implementing this information about the confidentiality of clients' information within the workplace.
    a. For the purpose of this Policy, the workplace, including electronic devices used in the course of business, and actions taken in the workplace, include, but are not limited to: records carried into a client's home, computers in the employee's or the volunteer's home with PHI, electronic devices that store or copy PHI, information kept in the employee's or volunteer's car and/or office, and any similar actions or locations.
3. Employees and volunteers are expected to comply with the Agency's rules, federal regulations related to HIPAA, and related state regulations, including the Texas HB 300, as well as changes from other applicable authorities.
    a. Compliance includes attending all of the Agency's trainings on HIPAA and the Texas HB 300.
    b. If an employee or volunteer discloses any clients' PHI or PII, s/he will be subject to the Agency's Progressive Discipline Policy, up to and including termination.
4. Documentation of the orientation and training will be kept in the individual's personnel file or in-service records.
    a. The Privacy Officer will be responsible for ensuring and documenting that the Governing Body, management team, employees, and volunteers receive the initial orientation, along with a copy of the Agency's Notice of Privacy Practices, as well as ongoing training for federal and state HIPAA-related compliance.

B. Additional non-computer related actions employees and volunteers will take to ensure the clients' privacy is protected include, but are not limited to:

1. Not talking about a client in front of another client or his/her representative or family;
2. Not using the client's telephone for personal calls or to call the office about another client;
3. Not using his/her personal cell phone to call the office from a client's home to talk about another client;
4. Conducting any discussion involving client information privately and discreetly to avoid disclosure to unauthorized employees or volunteers without a need-to-know;
5. Not calling out information in the office that might be considered personal such as the client's name and test results, medications, etc.;
6. Not calling out the client's name from desk-to-desk or over the intercom to announce s/he is calling;
7. Turning files over so someone without a need to know can't see the name on the file;
8. Not leaving files or folders open or unattended; and

9. Locking file cabinets and/or the record room for the security of records and to protect them from access and/or retrieval by unauthorized personnel.

**Procedure - Confidentiality in the Workplace**

A. The Security Officer will conduct an initial risk analysis of the Agency's systems containing PHI to ensure its security measures allow it to reasonably and appropriately comply with the HIPAA Security Rule, HITECH Rules, and the Texas HB 300.

1. In deciding if its security measures are adequate, the Security Officer may consider the following about the Agency:

   a. Its size, complexity, and capabilities;

   b. Its technical infrastructure, hardware, and software;

   c. The costs of the security measures; and

   d. The likelihood and possible impact of potential risks to PHI.

2. Periodically, the Security Officer will conduct risk analyses to evaluate the effectiveness of the Agency's security measures that have been put in place to find and/or mitigate any potential risks to the clients' PHI.

   a. A risk analysis will be completed following impermissible uses and disclosures of PHI by the Agency or a Business Associate.

3. The Security Officer will document the risk analyses findings and any actions taken to improve the security of the Agency's systems containing PHI, whether in a paper or electronic format.

   a. The Security Officer will make the documentation available to those responsible for implementing the findings and to appropriate regulatory entities.

   b. The Security Officer will review the documentation periodically and update it as needed in response to environmental or operational changes affecting the security of the clients' PHI.

   c. The Security Officer will retain the required documentation for seven (7) years from its creation or the date when it was last in effect, whichever is later.

B. The Agency will develop a Notice of Privacy Practices (Notice) containing the essential elements required by the HIPAA Standards.

1. The Notice of Privacy Practices will be given to the client or the client's representative as noted above in Procedure - Clients A.3.

2. The Notice of Privacy Practices will be displayed by posting the Notice:

   a. In a prominent place in the office where people seeking services may be able to read the Notice; and

   b. On the Agency's website.

C. Additional non-computer related actions the Agency will take to ensure the clients' privacy is protected include, but are not limited to:

1. Any information needing to be faxed will have a cover sheet stating the confidential nature of the information with procedures to be followed in case of a transmission received in error.
    a. The following information will not be faxed:
        i. Occurrence/Incidence Reports;
        ii. Employee Drug Screening Reports; and
        iii. Employee/Client HIV testing results.
2. Information collected during Quality Assurance Performance Improvement (QAPI) activities is confidential; but, it may be shared in statistical reporting formats.
3. Records will be located in such areas so as to avoid unofficial use or access by unauthorized persons.
4. Guidelines will be implemented as to when release and/or removal of clients' records is allowed and are in Policy IM.5 Record Information Release and Removal that is incorporated here by reference.
5. Guidelines for copying a client's record include, but are not limited to:
    a. The purpose for which the record is copied;
    c. Which portions of the record may be copied;
    d. The protection and security of the record by the employee/volunteer who made the copy; and
    e. The destruction of the copies.
6. Client information boards will not be displayed in common office areas that are viewable to the public.

**Procedure - Confidentiality Pertaining to Electronic Devices**

A. In addition to the privacy and security measures found throughout this Policy, the Agency will:
    1. Ensure the confidentiality, integrity, and availability of all PHI it creates, receives, maintains, or transmits;
    2. Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI;
    3. Protect against any reasonably anticipated uses or disclosures of PHI other than those that are permitted by the HIPAA Security Rule; and
    4. Secure written contracts that include confidentiality clauses, HIPAA Privacy Rule obligations, and breach notification requirements from:
        a. Persons that provide data transmission services with respect to PHI to the Agency and that require access on a routine basis to the PHI;
        b. Billing companies who are billing via electronic means; and
        c. Vendors offering client records to one or more individuals on behalf of the Agency.

5. Incorporate the PHI meaningful use concepts to:
    a. Improve quality, safety, efficiency, and to reduce health disparities;
    b. Engage clients and their families in improving their health;
    d. Improve care coordination;
    e. Improve public health; and
    f. Ensure adequate privacy and security protection for PHI.

B. The Security Officer will assign a login ID (user name) and password to each person authorized to have access to the Agency's electronic data.
    1. The Agency's computer data will be entered, accessed, or retrieved only by authorized persons.
    2. The Agency's computers, laptops, tablets, and other electronic devices will be locked when not in use and accessed only with the user's password.
    3. Passwords will be changed every three (3) months, after any untoward email encounter, and following any impermissible use (breach).
    4. Login IDs and passwords will not be shared, written down, or left in areas accessible to others.
    5. Authorized persons may utilize electronic signatures made and authenticated by the Agency's system to the extent the signature is valid under applicable law.
    6. Authorized persons will log off the electronic device at the end of the work session or whenever the device is not in his/her immediate possession.
    7. User access will be inactivated if the authorized person is on an extended leave of absence for more than thirty (30) days.
    8. Login IDs and passwords will be deleted and not used again when an authorized user is suspended, resigns, or is terminated.

C. Additional electronic device related actions the Agency may take to ensure the clients' privacy is protected include, but are not limited to:
    1. Installing high-quality firewalls and up-to-date virus protection software;
    2. Instructing users not to open email from unknown sources or unexpected email with attachments;
    3. Incorporating computer backup modalities (i.e. online, backup disks, CDs, hard drives, etc.) for critical performance;
        a. Computer data will be backed up daily.
        b. One version of the backup will be kept in a secure place offsite such as in a bank safe deposit box.
    4. Using surge protectors, uninterruptable power supplies, or other backup systems to protect computers during power outages and/or power surges;
    5. Installing and enabling encryption;

6. Not installing or, if present, disabling file sharing applications;
7. Turning computer screens away from public view, using privacy screens, or using screen savers to prevent unauthorized persons from viewing screens, intentionally or unintentionally;
8. Having an automatic logoff to ensure unauthorized persons do not access data on unattended electronic devices; and
9. Deleting and scrubbing devices with PHI before they are discarded.

D. Authorized persons will be permitted access to the minimum amount of client PHI necessary to perform their duties.

1. Administrative personnel, including Supervisors, may have access to all information 24 hours a day, 7 days a week.
2. Attendants may have access to client information at the office during office hours.
3. Billing personnel may have access to information needed to process claims at the office during office hours.

**Procedure - Confidentiality Pertaining to Business Associates**

A. The Agency will secure written contracts that include confidentiality clauses, Privacy Rule obligations, and breach notification requirements from its Business Associates and their subcontractors who create, receive, maintain, or transmit PHI.

B. The Agency's Business Associates shall have access to the minimum amount of client PHI needed to accomplish the cited purpose as noted in the contract.

C. The Agency's Business Associates, such as a Health Information Organization (HIO), may use and disclose PHI for its proper management and administration.

1. Data aggregation services related to the Agency's operations may be provided.

D. The Agency's Business Associates may authorize their subcontractors to make HIPAA compliant uses and disclosures just as the Agency is permitted to make.

E. The Business Associates are held to the same standards for breaches of information as the Agency is. In addition to the information that follows in the Breach section, the Business Associates and their subcontractors:

1. Are liable for their breaches;
2. Will notify the Agency of a breach without reasonable delay and not less than 60 days from the discovery of a breach;
3. Will be given an opportunity to correct any alleged material breach the Agency discovers within a specified period; and
4. Will have the contract terminated by the Agency if it determines there has been a violation of the HIPAA Security Rule, the Texas HB 300, or a breach of confidentiality.

**Procedure - Breaches**

A. In the event of an impermissible use or disclosure of PHI, the Security Officer or designee will provide notification to the Secretary of HHS per the HIPAA Breach Notification Rule unless the Security Officer determines there is a low probability the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature, extent, and identifiers of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.
5. The Security Officer will document and retain its risk assessment and determination.

B. There are three exceptions to the definition of the word "breach:"

1. The unintentional acquisition, access, or use of PHI by an employee or person acting under the authority of the Agency or Business Associate if such acquisition, access, or use was made in good faith and within the scope of his/her authority;
2. The inadvertent disclosure of PHI by a person authorized to access it at the Agency or Business Associate's to another person at the Agency or the Business Associate's who is authorized to access the PHI; and
3. The Agency or Business Associate has a good faith belief the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.
4. The Agency or Business Associate must ensure the information cannot be further used or disclosed in a manner not permitted by the HIPAA Privacy Rule.

C. The Agency will notify clients whose unsecured PHI has been breached as follows, taken directly from the Notification Requirements:

1. The Agency will provide the client with notice in written form by first-class mail, or alternatively, by e-mail if the client has agreed to receive such notices electronically.
2. If the Agency has insufficient or out-of-date contact information for ten (10) or more clients, the Agency will provide substitute individual notice by either posting the notice on the home page of its website for at least 90 days or by providing the notice in major print or broadcast media where the clients likely reside.
    a. The Agency will include a toll-free phone number that remains active for at least 90 days where clients can learn if their information was involved in the breach.
3. If the Agency has insufficient or out-of-date contact information for fewer than ten (10) clients, the Agency may provide substitute notice by an alternative form of written notice, by telephone, or other means.
    a. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.
    b. The individual notifications must include, to the extent possible:

i. A brief description of the breach;

ii. A description of the types of information that were involved in the breach;

iii. The steps affected clients should take to protect themselves from potential harm;

iv. A brief description of what the Agency is doing to investigate the breach, mitigate the harm, and prevent further breaches; and

v. Contact information for the Agency or the Business Associate, as applicable.

c. With respect to a breach by a Business Associate, while the Agency is ultimately responsible for ensuring clients are notified, the Agency may delegate the responsibility of providing the individual notices to the Business Associate.

i. The Agency and the Business Associate will consider which entity is in the best position to provide notice to the client, which may depend on various circumstances, such as the functions the Business Associate performs on behalf of the Agency and which entity has the relationship with the client.

4. If the Agency experiences a breach affecting the unsecured PHI of more than 500 clients in its licensure geographic service area, in addition to notifying the affected clients, it will provide notice in a press release to prominent media outlets serving that area.

a. This media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice described in 3b.

5. In case of a breach affecting the unsecured PHI of either more or less than 500 clients, the Agency will notify the Secretary of HHS by visiting the HHS website, filling out the breach report form, and electronically submitting the form.

a. If the breach affects 500 or more clients, the Agency will notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

b. If the breach affects fewer than 500 clients, the Agency may notify the Secretary of such breaches on an annual basis.

i. Reports of breaches affecting fewer than 500 clients are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

6. If a breach of unsecured PHI occurs by a Business Associate, it must notify the Agency without unreasonable delay and no later than 60 days from the discovery of the breach.

a. To the extent possible, the Business Associate should provide the Agency with the identification of each client affected by the breach, as well as any other available information required to be provided by the Agency in its notification to the affected clients.

7. The Agency and its Business Associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach.

a. Accordingly, with respect to an impermissible use or disclosure, the Agency or its Business Associate will maintain documentation that all required notifications were made, or, alternatively, will maintain documentation to demonstrate that notification was not required because:

i. Its risk assessment demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure; or

ii. The application of any other exceptions to the definition of "breach."

**Website Resources:**

Breach notifications - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Breach notification rule - http://thefederalregister.com/2009/04/20/E9-8882.html

HITECH Act - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Summary of the HIPAA Privacy Rule -

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Summary of the HIPAA Security Rule -

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Texas House Bill (HB) 300 (Enrolled) - https://capitol.texas.gov/BillLookup/Text.aspx?LegSess=82R&Bill=HB300