Faithful Steps
Therapy Solutions of the Big Country

HIPAA PRIVACY & SECURITY PLAN

March 2025

TABLE OF CONTENTS

HIPAA Privacy & Security Plan

ATTACHMENTS

HIPAA Privacy & Security Plan

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict Faithful Steps Therapy Solutions (“Faithful Steps”, “Clinic”) abilities to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Clinic and relates to the past, present, or future physical or mental health condition of a Patient/Client (“Participant”); the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

Some examples of PHI are:

- Participant’s medical record number
- Participant’s demographic information (e.g. address, telephone number)
- Information doctors, nurses and other health care providers put in a participant’s medical record
- Images of the participant
- Conversations a provider has about a participant’s care or treatment with nurses and others
- Information about a participant in a provider’s computer system or a health insurer’s computer system
- Billing information about a participant at a clinic
- Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual

It is the Clinic’s policy to comply fully with HIPAA's requirements. To that end, all staff members who have access to PHI must comply with this HIPAA Privacy and Security Plan. For purposes of this plan and the clinic’s use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, interns, board members and other persons whose work performance is under the direct control of Faithful Steps, whether or not they are paid by Faithful Steps. The term "employee" or “staff member” includes all of these types of workers.

No third-party rights (including but not limited to rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan. Faithful Steps reserves the right to amend or change this Plan at any time (and even retroactively) without notice.

All staff members must comply with all applicable HIPAA privacy and information security policies. If after an investigation you are found to have violated the organization’s HIPAA privacy and information security policies, then you will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

SECTION 1: Responsibilities as Covered Entity

I. Privacy Officer

The Operations Director will be the HIPAA Privacy Officer for Faithful Steps Therapy Solutions. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Clinic's use and disclosure procedures. The Privacy Officer will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI. The Privacy Officer can be reached at (325) 268-4052.

II. Incident Response Team

The Incident Response Team is comprised of the Privacy Officer, Clinical Director, and additional members deemed appropriate on an ad hoc basis in the reasonable judgment of the Privacy Officer. In the event of a security incident that results in a wrongful disclosure of PHI, the Privacy Officer, in conjunction with the Incident Response Team will take appropriate actions to prevent further inappropriate disclosures. In addition, Human Resources and Legal may be consulted as part of the review team to assist in the review and investigation of privacy incidents when required. If the Privacy Officer and Incident Response Team have not resolved the incident, the Privacy Officer shall involve anyone determined to be necessary to assist in the resolution of the incident. If participants need to be notified of any lost/stolen PHI, the Privacy Officer will send PHI Theft/Loss Disclosure Letters to all possible affected individuals.

III. Workforce Training

It is the Clinic's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. All staff members receive HIPAA training. Whenever a privacy incident has occurred, the Privacy Officer in collaboration with management will evaluate the occurrence to determine whether additional staff training is in order. Depending upon the situation, the Privacy Officer may determine that all staff should receive training that is specific to the privacy incident. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the Clinic's privacy policies and procedures.

IV. Safeguards

The Clinic has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets and periodically changing door access codes. Additionally, all staff members can only access PHI by using their own login information.

Firewalls ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

Data Storage / Backup / Remote Access

Currently all data in the local data Clinic is backed up using industry standards with off-site storage of media. Faithful Steps currently utilizes technology that allows for quickly removing, disabling, and starting staff member access to PHI.

V. Privacy Notice

The Privacy Officer is responsible for developing and maintaining a notice of the Clinic's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Clinic;
- the individual's rights; and
- the Clinic's legal duties with respect to the PHI.

The privacy notice will inform participants that the Clinic will have access to PHI. The privacy notice will also provide a description of the Clinic's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants:

- on an ongoing basis, at the time of an individual's enrollment into a Clinic program or at the time of treatment and consent; and
- within 60 days after a material change to the notice.

The Clinic will also provide notice of availability of the privacy notice at least once every three years.

VI. Complaints

The Privacy Officer will be the Clinic's contact person for receiving complaints. The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Clinic's privacy procedures and for creating a system for handling such complaints. A copy of the complaint form shall be provided to any participant upon request.

VII. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Plan will be imposed in accordance up to and including termination.

VIII. Mitigation of Inadvertent Disclosures of Protected Health Information

Faithful Steps shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of a Participant's PHI in violation of the policies and procedures set forth in this Plan. As a result, if an employee becomes aware of a disclosure of protected health information, either by a staff member of the Clinic or an outside consultant/contractor that is not in compliance with this Policy, immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

IX. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

X. Plan Document

The plan document includes provisions to describe the permitted and required uses and disclosures of PHI by Faithful Steps. Specifically, the plan document requires Faithful Steps to:

• not use or further disclose PHI other than as permitted by the plan documents or as required by law;

• ensure that any agents or subcontractors to whom it provides PHI received from the Clinic agree to the same restrictions and conditions that apply to Faithful Steps;

• report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;

• make PHI available to Participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures;

• make the Clinic's internal practices and records relating to the use and disclosure of PHI received by the Clinic available to the Department of Health and Human Services (DHHS) upon request; and

XI. Documentation

The Clinic's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

Faithful Steps shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

Incident Report

The Clinic has developed an Incident Report form. This form is used to document reports of privacy breaches that have been referred to the Privacy Officer from staff members who have reviewed or received the suspected incident.

After receiving the Incident Report form from staff members, the Privacy Officer classifies the incident and its severity and analyzes the situation. Documentation shall be retained by the Clinic for a minimum of six years from the date of the reported incident.

If the Privacy Officer is able to resolve the incident, the Privacy Officer shall also document the actions taken to resolve the issue in the Incident Report form.

XII. Electronic Health Records

Just like paper records, Electronic Health Records must comply with HIPAA, and other state and federal laws. Unlike paper records, electronic health records can be encrypted - using technology that makes them unreadable to anyone other than an authorized user - and security access parameters are set so that only authorized individuals can view them. Further, EHRs offer the added security of an electronic tracking system that provides an accounting history of when records have been accessed and who accessed them.

XIII. Access Authorization

Faithful Steps will grant access to PHI based on their job functions and responsibilities.

The Privacy Officer is responsible for the determination of which individuals require access to PHI and what level of access they require through discussions with the individual's manager and or department head.

The Operations Director will keep a record of authorized users, the rights that they have been granted with respect to PHI, and will keep a comprehensive matrix of how and to who rights are granted.

SECTION 2: Use and Disclosure of PHI

I. Use and Disclosure Defined

The Clinic will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Clinic, or by a Business Associate of the Clinic.

- *Disclosure.* For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within Faithful Steps with a business need to know PHI.

II. Access to PHI Is Limited to Certain Employees

All staff who performs Participant functions directly on behalf of the Clinic or on behalf of group health plans will have access to PHI as determined by their department and job description and as granted by the Operations Director.

These employees with access may use and disclose PHI as required under HIPAA but the PHI disclosed must be limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved compliant authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

Staff members may not access either through our information systems or the participant's medical record the medical and/or demographic information for themselves, family members, friends, staff members or other individuals for personal or other non-work related purposes, even if written or oral participant authorization has been given. If the staff member is a Participant in Faithful Steps's plans, the staff member must go through their Provider in order to request their own PHI.

In the very rare circumstance when a staff member's job requires him/her to access and/or copy the medical information of a family member, a staff member, or other personally known individual, then he/she should immediately report the situation to his/her manager who will determine whether to assign a different staff member to complete the task involving the specific Participant.

Your access to your own PHI must be based on the same procedures available to other participants not based on your job-related access to our information systems. For example, if you are waiting for a lab result or want to view a clinic note or operative report, you must either contact your physician for the information or make a written request to the Privacy Officer. You cannot access your own information; you must go through all the appropriate channels as any Participant would have to.

III. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

I. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Clinic's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. Permitted are disclosures:

• about victims-of abuse, neglect or domestic violence;

• for judicial and administrative proceedings;

• for law enforcement purposes;

• for public health activities;

• for health oversight activities;

• about decedents;

• for cadaver organ, eye or tissue donation purposes;

• for certain limited research purposes;

• to avert a serious threat to health or safety;

• for specialized government functions; and

• that relate to workers' compensation programs.

II. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

The "minimum-necessary" standard does not apply to any of the following:

• uses or disclosures made to the individual;

• uses or disclosures made pursuant to a valid authorization;

• disclosures made to the Department of Labor;

• uses or disclosures required by law; and

• uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For making disclosures of PHI to any business associate or providers, or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.

All other disclosures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making *requests* for disclosure of PHI from business associates, providers or participants for purposes of claims payment/adjudication or internal/external auditing purposes, only the minimum necessary amount of information will be requested.

All other requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

I. Disclosures of PHI to Business Associates

With the approval of the Privacy Officer and in compliance with HIPAA, employees may disclose PHI to the Clinic's business associates and allow the Clinic's business associates to create or receive PHI on its behalf. However, prior to doing so, the Clinic must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate contract is in place.

Business Associate is an entity that:

• performs or assists in performing a Clinic function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or

• provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Examples of Business Associates are:

- A third party administrator that assists the Clinic with claims processing.
- A CPA firm whose accounting services to a health care provider involves access to protected health information.
- An attorney whose legal services involve access to protected health information.
- A consultant that performs utilization reviews for the Clinic.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of the Clinic and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services for the Clinic.
- A pharmacy benefits manager that manages a health plan's pharmacist network.

II. Disclosures of De-Identified Information

The Clinic may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

18 specific elements listed below - relating to the participant, employee, relatives, or employer - must be removed, and you must ascertain there is no other available information that could be used alone or in combination to identify an individual.

1. Names
2. Geographic subdivisions smaller than a state
3. All elements of dates (except year) related to an individual - including dates of admission, discharge, birth, death - and for persons >89 y.o., the year of birth cannot be used.
4. Telephone numbers
5. FAX numbers
6. Electronic mail addresses
7. Social Security Number
8. Medical Record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plates
13. Device identifiers and serial numbers
14. Web URLs
15. Internet protocol addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photos, and comparable images

18. Any unique identifying number, characteristic or code

A person with appropriate expertise must determine that the risk is very small that the information could be used alone or in combination with other reasonably available information by an anticipated recipient to identify the individual. AND this person must document the methods and justification for this determination.

I. Disclosures to Family, Friends or Others-Participant Location

There are instances when a participant's friend or family member contacts Faithful Steps to ask about the location of a patient or whether the patient has been seen at Faithful Steps. Following is guidance provided to assist staff in providing appropriate responses for specific situations that commonly occur. In rare cases of emergency, at the discretion of senior management the minimum of information may be released in order to assist in resolving an emergency situation.

Guidance

Situation: Friends or family are concerned about the whereabouts of a person. They contact the Clinic to ask if a person is at Faithful Steps or has been seen as a participant recently.

Response:
If the person is not currently a Faithful Steps participant, the caller may be told that the person is not at the clinic. If the person is currently receiving services at the clinic, clinic staff should take the name of the caller, their purpose for calling the participant and tell them that they will check. Staff should then ask the participant if it is okay to provide information to the caller and what information to provide. If the patient does not want the clinic staff to provide information, staff should tell the caller that they are unable to provide information about the participant due to privacy rights and suggest that the caller contact the participant directly for information.
If the caller is asking for historical information about visits or services provided and the participant has not either provided an authorization to share this information with this person pertaining to their involvement in the patient's treatment or payment, the caller should be informed that due to HIPAA confidentiality requirements, information about participant visits is not provided without participant authorization.

Situation: **An individual comes to Faithful Steps and tells the reception area that they have arrived to pick up a patient.**

Response:
If the participant has notified Faithful Steps staff that someone is coming to pick them up (by giving the name of the individual), the individual should be directed to the location of the participant. If the patient has not provided information about anyone coming to pick them up, Faithful Steps staff should ask for the person's name and tell the person that they will check. Another staff member should be given a note to tell the participant that someone has arrived to pick them up and ask them whether it is okay to tell the person the participant's location.

I. Removing PHI from Clinic Premises

When Faithful Steps deems it necessary for an employee to work from a location other than one of our sites, PHI may be accessed and/or removed under the following circumstances:

1. Before removing PHI from Faithful Steps for Clinic business you must receive the approval from your department Director.

2. Faithful Steps will only allow the paper (participant records, reports) removal of PHI when transported in a secure lock box and when approved by the department Director and the Privacy Officer.
3. Staff members that work at school sites and create paper files at the school are required to keep these files locked securely.
4. Staff member with progress notes and other forms that need to be signed by their supervisors can be brought back to Faithful Steps in a locked carrying case. These documents can also be saved on the Faithful Steps server in a designated secure file on the Clinic network, or on a password-protected flash drive.
5. The electronic removal of PHI (using flash drives) for the purposes of working from a non-Faithful Steps setting may be approved in advance by the Operations Director only. In the very rare circumstance that it becomes necessary, the PHI should be rigorously safeguarded physically as well as electronically, including *employee-performed* encryption of all files. Most flash drives have the capability to assign a password.
6. The following safeguards are required of all employees when working from a non-Faithful Steps site:
    - When outside the facility, only work on health information in a **secure private environment.**
    - Keep the information with you **at all times** while in transit.
    - Do not permit others to have access to the information.
    - Never email participant information.
    - Don't save participant information to your home computer.
    - Do not print records of any type.
    - Do not record login information on or near the computer.
    - Return all information the next business day or as soon as required.

Faithful Steps will immediately investigate any incident that involves the loss or theft of PHI that was taken off-site.

II. Faxing PHI

Each fax should be accompanied by an Faithful Steps fax cover sheet. Faxing of highly confidential information is not recommended. Faxing of highly confidential information is only permitted if the sender first calls the recipient and confirms that the recipient or his/her designee can be waiting at the fax machine, and then, the recipient or his/her designee waits at the fax machine to receive the fax and then calls the sender to confirm receipt of the document. Both the sender and the recipient must be attentive to the sensitive nature of highly confidential information.

If the fax was transmitted to the wrong recipient, in all cases follow these steps:

Fax a request to the incorrect fax number explaining that the information has been misdirected and ask that the materials be returned or destroyed. Document the incident on an Incident Report Form and notify the HIPAA Privacy Officer at (325) 268-4052. Verify the fax number with the recipient before attempting to fax the information again.

SECTION 3: Participant Individual Rights

I. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Clinic or its business associates maintains. HIPAA also provides that participants may request to have their PHI amended. The Clinic will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

II. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

• to carry out treatment, payment or health care operations;

• to individuals about their own PHI;

• incident to an otherwise permitted use or disclosure or pursuant to an authorization;

• for purposes of creation of a facility directory or to persons involved in the participant's care or other notification purposes;

• as part of a limited data set; or

• for other national security or law enforcement purposes.

The Clinic shall respond to an accounting request within 60 days. If the Clinic is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings. The Privacy Officer is responsible for responding to a request for Accounting.

III. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of Faithful Steps, the requests are reasonable.

However, Faithful Steps shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Officer in collaboration with managers has responsibility for administering requests for confidential communications.

I. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Clinic’s policy to attempt to honor such requests if, in the sole discretion of the Clinic, the requests are reasonable. The Privacy Officer is charged with responsibility for processing requests for restrictions.

II. When a Participant Requests a Copy of his/her Record

A participant can request a copy of his/her medical record by completing a Request for Accessing/Inspecting/Copying Health Information form and submitting it to the Department that maintains the information being requested. The Department in collaboration with the Privacy Officer must process and respond to the request.

Participants can receive this form from Patient Services or by going directly to the department that maintains their records.

III. Participants Request for copy of Clinic Notes or Labs while Checking out After an Appointment

It's okay to provide a participant with a copy of a clinic note or labs that are maintained in their files. It is recommended that you follow the best practice of stamping or writing "Participant Copy" on **each** page.

IV. Acceptable Methods of Verification of Identity for Release of Personal Health Information (PHI):

When the Requestor is the Participant

The Clinic will take reasonable steps and exercise professional judgment to verify the identity of the individual making a request for access to his/her own PHI.

a. **If the request is made in person**, verification of identity may be accomplished by asking for photo identification (such as a driver's license). A copy of the I.D. must be attached to the request and placed in the Participants record.

b. **If the request is made over the telephone**, verification will be accomplished by requesting identifying information such as social security number and birth date and confirming that this information matches what is in the participant's record. Or, verification will occur through a callback process using phone numbers documented in the participant record to validate the caller's identity.

c. **If the request is made in writing,** verification will be accomplished by requesting a photocopy of photo identification. If a photocopy of the ID is not available, the signature on the written request must be compared with the signature in the participant record. In addition, Faithful Steps will need to verify the validity of the written request by contacting the participant by telephone.

V1II. When the requestor is the Participants Legally Authorized Representative

Verification of identity will be accomplished by asking for a valid photo identification (such as driver's license) if the request is made in person. Once identity is established, authority in such situations may be determined by confirming the person is named in the medical record or in the participant's profile as the participant's legally authorized representative. Or, if there is no person listed in the medical record as the participant's legally authorized representative, authority may be established by the person presenting an original of a valid power of attorney for health care or a copy of a court order appointing the person guardian of the participant and a valid photo I.D. A copy of the I.D. and legal notice must be attached to the request and placed in the Participants record.

IX. Other Methods

The Clinic may use any other method of verification that, in the Clinic's discretion, is reasonably calculated to verify the identity of the person making the request. Some acceptable means of verification include, but are not limited to:

a. Requesting to see a photo ID
b. Requesting a copy of a power of attorney
c. Confirming personal information with the requestor such as date of birth, policy number or social security number
d. Questioning a child's caretaker to establish the relationship with the child
e. Calling the requestor back through a main organization switchboard rather than a direct number

PHI Breach Reporting

The purpose of this section is to address the Clinic's privacy requirements for reporting, documenting, and investigating a known or suspected action or adverse event resulting from unauthorized use or disclosure of individually identifiable health information.

A privacy breach is an adverse event or action that is unplanned, unusual, and unwanted that happens as a result of non-compliance with the privacy policies and procedures of the Clinic. A privacy breach must pertain to the unauthorized use or disclosure of health information, including 'accidental disclosures' such as misdirected e-mails or faxes.

The Privacy Officer shall immediately investigate and attempt to resolve all reported suspected privacy breaches.

Staff members are required to verbally report to his/her supervisor any event or circumstance that is believed to be an inappropriate use or disclosure of a participant PHI. If the supervisor is unavailable, the staff member must notify the Privacy Officer within 24 hours of the incident. If the manager determines that further review is required, the manager and staff member will consult with the Privacy Officer to determine whether the suspected incident warrants further investigation. In all cases an Incident Report must be filled out and submitted to the appropriate reviewer.

The Privacy Officer will document all privacy incidents and corrective actions taken. Documentation shall include a description of corrective actions, if any are necessary, or explanation of why corrective actions are not needed, and any mitigation undertaken for each specific privacy incident. All documentation of a privacy breach shall be maintained with the Privacy Officer and shall be retained for at least six years from the date of the investigation. Such documentation is not considered part of the participant's health record.

If the participant is not aware of a privacy incident, the Privacy Officer shall investigate the incident thoroughly before determining whether the participant should be informed. If the participant is aware of a privacy incident, the Privacy Officer shall contact the participant within three (3) business days of receiving notice of the incident. The method of contact is at the discretion of the Privacy Officer but resulting communications with the participant must be documented in the incident report. In addition, any privacy incident that includes a

disclosure for which an accounting is required must be documented and entered into accounting.

Staff who fail to report known PHI/security incidents, or fail to report them promptly, may be subject to disciplinary action up to termination.

I. Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals if necessary and in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by

first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

Media Notice

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, 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.

Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60

days after the end of the calendar year in which the breaches occurred.

Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

I. Complaint/Concerns Reporting

Concerns about the Clinic's privacy practices may arise in a variety of contexts and may be received by many different persons at the Clinic. It is important that the Clinic responds to concerns and complaints in a timely manner. When a staff member hears or receives a complaint/concern, he/she should ask the complainant whether or not the complainant wishes to file a formal complaint and offer to assist the complainant with the form. Even if the person does not wish to file a complaint or provide identifying information, the staff member should proceed with the procedures outlined below.

Filing a Complaint

a. **Participant's** complaints of alleged privacy rights violations may be forwarded through multiple channels, such as telephone calls, letter via mail/email, in person. If these complaints are received by a staff member the person receiving the complaint will:

- In response to a Telephone Call or In-Person Request to File a Complaint – Complete the Privacy Complaint Form and immediately forward to the Privacy Officer. Offer to forward a copy of the complaint form to the complainant.
- In response to a Letter or Email (print out) – Complete the Privacy Complaint Form and immediately forward to the Privacy Officer. Attach the written complaint to the complaint form.
- In response to an Anonymous Complaint– Complete the Privacy Complaint Form based on the information provided and immediately forward to the Privacy Officer. When possible, explain to the complainant that the Clinic has an obligation to follow up on complaints whether or not they are anonymously filed.

b. **Staff Members** – Call the Privacy Officer at (325) 268-4052. Staff members may also complete the Privacy Complaint Form and forward to the Privacy Officer. Staff members can also fill out the complaint form and put it in the Privacy Officers mail box located at 3444 N 1st St, Ste 508, Abilene, TX 79603. Upon receipt of a complaint, the Privacy Officer will initiate primary investigation.

- **Initial review** – All complaints will be initially reviewed by the Privacy Officer or his/her designee to determine if the complaint alleges a violation of established policies and procedures or other known regulations regarding the protection of individually identifiable health information. If there is no legitimate allegation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of this finding within 60 days. All documentation will be maintained as prescribed in this policy.
- **Complaints requiring further review** – If there is a legitimate allegation, the Privacy Officer or his/her designee will conduct a detailed investigation by reviewing the covered Clinic practices, contacting employees, students, or volunteers as needed, working with the Security Officer (as applicable), and utilizing other Clinic resources as needed. Upon conclusion of the investigation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of the finding within 60 days.

c. **60-day time frame –** In the event that this 60-day period cannot be met, the Privacy Officer shall, when possible, communicate this determination to the Complainant in writing and include an estimated timeframe for completion of the investigation.

d. **Outcome of Investigation -** The purpose of the investigation is to determine the compliance of the Clinic's policies and procedures implementing the privacy standards mandated by HIPAA. The Clinic will mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of PHI in violation of the Clinic's policies and procedures or HIPAA's privacy requirements by the Clinic or any of its Business Associates. In the event that disciplinary action is recommended, the Privacy Officer or his/her designee will coordinate any action with management.

e. **Documentation -** All complaints sent to the Privacy Officer shall be documented in a format that includes all of the information contained on the Privacy Complaint Form. The Privacy Officer will maintain all completed complaints' documentation for six years from the initial date of the complaint.

I. Non-Retaliation

The Clinic shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident.

ATTACHMENTS

Summary Guidelines for Safeguarding the Privacy of Health Information

These are guidelines on how to safeguard health information and ensure confidentiality when using normal business communications, such as conversations, telephone, faxes, mail, and electronic mail. Wherever practical, the material containing Protected Health Information (PHI) should be labeled as confidential on the document, diskette, CD, or other medium. PHI maintained electronically should be password-protected in all media.

Also when using and disclosing PHI, you must take reasonable measures to ensure the information is protected. Below are simple safeguarding tasks that should be used when communicating in a work environment that necessitates access to and use and disclosure of PHI. Remember to limit your communications of PHI to the minimum necessary for the intended purpose. Restrict your communications to those who have a valid "need to know" the information. If you have questions about these safeguards and how to protect PHI communications, please discuss them with your supervisor.

Oral Conversations – in person

□ Discuss participants PHI in private. Use an office with a door whenever possible, or leave areas where others can overhear.

□ Be aware of those around you and lower your voice when discussing participants health information.

□ If possible, point out health information on paper or on-screen non- verbally when discussing participants health information.

Oral Conversations - telephone

□ Follow the above guidelines for "Oral Conversations"-in person"

□ Don't use names instead say; "I have a question about a client".

□ Never give PHI over the phone when talking to unknown callers, but call back and verify information.

□ Never leave PHI on voice messages; instead leave a message requesting a return call to discuss a participant giving only your name and phone number.

□ Do not discuss PHI over unencrypted cellular or portable (wireless) phones or in an emergency, as the transmissions can be intercepted.

Fax

□ Put fax machines in a safe location, not out in the open or in a public or area with high-traffic or easy access and visibility.

□ Use a cover sheet clearly identifying the intended recipient and include your name and contact information on the cover sheet.

□ Include a confidentiality statement on the cover sheet of faxes that contain PHI.

□ Do not include or reference PHI on cover sheet.

□ Confirm fax number is correct before sending.

□ Send fax containing participant health information only when the authorized recipient is there to receive it whenever possible.

□ Verify that fax was received by authorized recipient; check the transmission report to ensure correct number was reached and when necessary contact the authorized recipient to confirm receipt.

□ Deliver received faxes to recipient as soon as possible. Do not leave faxes unattended at fax machine.

Email

□ Do not include PHI in Subject-line or in Body of email.

□ Transmit PHI only in a password-protected attachment (MS Word and MS Excel provide password protection).

□ Include a confidentiality statement on emails that contain any PHI in email attachments.

□ Do not send attachment passwords in the same email as the attachment.

□ Include your contact information (name and phone number minimum) as part of the email.

□ Set email sending options to request an automatic return receipt from your recipient(s).

□ Request that email recipients call to discuss specific participant data.

□ Do not store emails or email attachments with PHI on your hard drive but copy and store to a secure server. Delete the email and the attachments when they are no longer needed.

Courier and Regular Mail

□ Use sealed secured envelopes to send PHI.

□ Verify that the authorized person has received the package.

□ Deliver all mail promptly to the recipient.

□ Mailboxes must be in safe areas and not located in public or high-traffic areas.

Inter-Office Mail

□ Put PHI in closed inter-office envelopes. As an added precaution, put PHI in a sealed envelope inside the inter-office envelope.

□ Identify recipient by name and verify mail Clinic address.

□ Distribute inter-office mail promptly to recipients. Do not leave unattended in mailboxes.

□ Where practical, use lockable containers (e.g. attaches) to transmit correspondence that contains participant PHI.

Computer Workstations

□ Use password protected screen savers, turn off the computer, or log out of the network when not at your desk.

□ Position screens so they are not visible to others.

□ Secure workstations and laptops with password.

□ Change passwords on a regular basis.

□ Do not leave laptop or work-related participant PHI visible or unsecured in a car, home office, or in any public areas.

□ Ensure that all PHI used outside work premises is protected using appropriate measures such as locked desks, file cabinets.

□ Never remove original copies of PHI from the agency without your supervisor's approval for specific purposes.

□ Store files that contain PHI on a secure server, not on your workstation hard drive.

Disposal of PHI

□ Shred all hard copies containing PHI when the copies are no longer needed.

□ Place hardcopies to be recycled in locked recycle bins if available.

□ Delete all soft copy files containing PHI from your computer and from the server when the information is no longer needed within the record retention requirements.

□ Destroy all disks, CDs, etc., that contained PHI before disposing them.

□ Do not reuse disks, CDs that contained PHI without sanitizing them first.

□ Contact IT before transporting or transferring equipment for proper procedures to move equipment and to sanitize hard drives and other media.

□ Return the PHI to the sender, if this requirement is stipulated in any contractual agreements.

Work Areas

□ Do not leave PHI (files, records, Rolodex, reports) exposed, open, or unattended in public areas, conference rooms, mailboxes, wall trays, etc.

□ Store all PHI securely in locked file cabinets, desk drawers, offices, or suites when you are not in your work area.

Faithful Steps Therapy Solutions of the Big Country

SUMMARY NOTICE OF PRIVACY PRACTICES

THIS NOTICE OF PRIVACY PRACTICES DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY. THIS NOTICE IS BEING PROVIDED TO YOU PURSUANT TO FEDERAL LAW.

Your Protected Health Information (PHI)

"***Protected health information***" (PHI) is information about you, including demographic information, that may identify you or be used to identify you, and that relates to your past, present or future physical or mental health or condition, the provision of health care services, or the past, present or future payment for the provision of health care. Each time you have contact with a healthcare provider for delivery of healthcare, a record of your contact/visit is prepared. Your medical record is the physical property of Faithful Steps Therapy Solutions of the Big Country (Faithful Steps), but you have certain rights to restrict, or request restrictions on, some of the uses or disclosures of the information in your medical record, as further described in this Notice. However, Faithful Steps has the right to use and disclose the information contained in your medical record in the process of providing treatment, seeking or receiving payment, and performing other regular health care operations, as is further described herein.

Your Rights Regarding Your PHI

Except as otherwise provided by applicable law, you have the right to:

Inspect and copy your PHI and other medical records

- You may request to inspect or receive a copy of your PHI or other medical records about you that are maintained in a designated record set.
- So long as we maintain the requested information in the designated record set, we will provide you with a copy or summary of such information. We may charge a reasonable, cost-based fee for providing such information.

Request an amendment to your PHI and other medical records

- You may request that Faithful Steps amend PHI or other medical records about you in a designated record set that you believe to be incomplete or inaccurate.
- Faithful Steps is ***not*** required to change any such information if Faithful Steps deems such information to be accurate or if the information was provided from another source.
- If Faithful Steps does not change any such information, it will provide you with the reason for not doing so in a timely manner.

Request confidential communications

- You may request in writing to receive confidential communications from Faithful Steps regarding your PHI or other medical records.
- Faithful Steps will agree to all reasonable requests of this nature.

Request restrictions on the uses or disclosures of PHI

- You may request that Faithful Steps restrict uses or disclosures of your PHI in connection with treatment, payment, or health care operations. Faithful Steps is not required to agree to such a restriction. However, to the extent that Faithful Steps does agree with your request, Faithful Steps may not use or disclose the protected

PHI in violation of the restriction unless the PHI is needed to provide emergency treatment or is otherwise permitted or required by law.

- If you pay for a service or health care item out-of-pocket in full, you can ask Faithful Steps not to share that information for the purpose of payment or our operations with your health insurer. Faithful Steps will say "yes" unless a law requires us to share that information.

Receive an accounting of PHI disclosures

- You may ask for a list (an accounting) of the times Faithful Steps has shared your PHI for reasons other than treatment, payment, healthcare operations, or other disclosures you requested us to make during the six (6) years prior to the date of request, along with the persons or entities with whom the PHI was shared and the reasons for such disclosure.
- Faithful Steps will provide one (1) accounting per twelve (12) month period free of charge but will charge you a reasonable, cost-based fee if you ask for another accounting within twelve (12) months.

Receive a copy of this Notice

- You may request to receive a paper copy of this Notice at any time, even if you have agreed to receive the Notice electronically. We will provide you with a paper copy of the Notice in a prompt and timely manner.

Choose someone to act for you

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.

Additional rights; Complaint procedures

- Faithful Steps is required by law to maintain the privacy and confidentiality of your PHI and to provide you with notice of its legal duties and privacy practices with respect to such health information.
- Faithful Steps is also required by law to abide by the terms of this Notice, allow you to review this Notice prior to granting assent, and notify you of any changes and revisions to this Notice.
- If you believe that your privacy rights have been violated, you may submit a written complaint to Faithful Steps by contacting us at rgoulet@faithfulstepsbigcountry.com.
- You may also file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/.
- Faithful Steps will not retaliate against you in the event that you file a complaint.

<u>Your Choices</u>

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions. In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends, or others involved in your care

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases we never share your information unless you give us written permission:

- Sharing of therapy session notes

Our Uses and Disclosures of PHI

Faithful Steps may use and share your PHI and other health information in connection with providing treatment, receiving payment for health services, and performing other regular health operations such as:

- Documenting and describing the care you received for legal purposes;
- Communicating with other healthcare providers who may be involved in your care;
- Educating health care professionals;
- Conducting medical research;
- Providing information for government and public health entities responsible for improving public health and welfare;
- Evaluating and improving the care you receive and the outcomes achieved;
- Billing and verification of services provided to you; and
- Conducting other routine healthcare operations such as quality improvement studies and assessing healthcare provider competence.

Examples of Uses and Disclosures of Your PHI

We typically use or share your health information in the following ways.

Healthcare Delivery and Treatment

Information obtained from you by a physician, nurse, or other healthcare professional is documented in your record and used for the assessment, evaluation, diagnosis, and treatment of your medical condition(s). Following your treatment, this information may be provided to other healthcare professionals who may be involved in your care, such as other physicians, specialists, physical therapists, hospital-based providers, and/or other healthcare providers.

Example: Your physician and a Faithful Steps provider may need to coordinate your care.

Billing and Payment

Your PHI is utilized to justify the level of care delivered to you and the charges incurred for the services. This information generally accompanies the bill and is sent to our payers.

Example: We give information about you to your health insurance plan so it will pay for your services.

Healthcare Operations

Faithful Steps may disclose your PHI to other individuals and businesses in order to perform day-to-day operations. These other individuals and businesses include business associates such as vendors and/or contractors used for billing and claims management, medical research, disease management, and quality improvement initiatives, as well as management services organizations, laboratories, other free-standing diagnostic facilities, and legal counsel. Faithful Steps requires all business associates to agree to appropriately protect the confidentiality of your PHI.

Example: We use health information about you to manage the way we provide your treatment and services.

How else can we use or share your health information?

Faithful Steps is allowed or may be required to share your PHI or other health information in other ways – usually in ways that contribute to the public good, such as public health and research, which are summarized below. Faithful Steps has to meet many conditions in the law before we can share your information for these purposes. For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

To help with public health and safety issues

Faithful Steps can share health information about you for certain situations such as:

- Reporting suspected abuse, neglect, or domestic violence
- Preventing or reducing a serious threat to anyone's health or safety

To conduct research

Faithful Steps can use or share your information for health research where permitted by law or with your consent.

To comply with the law

Faithful Steps will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that Faithful Steps is complying with federal privacy law.

For Reminders and Treatment

Faithful Steps may contact you to provide you with information Faithful Steps feels is useful or helpful to you, based on your PHI. For example, Faithful Steps may contact you (or instruct a specialist provider to whom you have been referred to contact you) to schedule an appointment or as an appointment reminder, to suggest alternative treatments, or to provide you with information on treatments you are already receiving.

For Legal Reasons

We can use or share health information about you:

- For workers' compensation claims;
- For law enforcement purposes or with a law enforcement official;
- With health oversight agencies for activities authorized by law;
- For special government functions such as military, national security, and presidential protective services; or
- In response to a court or administrative order.

Other Miscellaneous Uses

- Faithful Steps may also utilize or disclose your PHI in order to communicate with or notify family members, relatives, and others responsible for your health, and funeral directors.
- Faithful Steps may disclose your PHI through other communications and reports required to be made by healthcare professionals, such as the public health department, law enforcement, the Food and Drug Administration, organ procurement organizations, correctional institutions, and workers compensation, where applicable.

- Other uses and disclosures of PHI not permitted or required by law will be made only with your written authorization. You may revoke your authorization at any time, provided that the revocation is in writing, except to the extent that Faithful Steps has already taken action in reliance on your prior authorization.

Our Responsibilities

- Faithful Steps is required by law to maintain the privacy and security of your protected health information.
- Faithful Steps will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- Faithful Steps must follow the duties and privacy practices described in this Notice and give you a copy of it.
- Faithful Steps will not use or share your health information other than as described here unless you permit otherwise in writing. If you authorize Faithful Steps to use or share your health information for additional purposes, you may revoke such additional authorization at any time in writing.

For more information, see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

Changes to the Terms of this Notice

Faithful Steps may change the terms of this Notice, and the changes will apply to all information Faithful Steps has about you. The new Notice will be available upon request, in our office, and on our website, www.faithfulstepsbigcountry.com.

Acknowledgement

I hereby acknowledge receiving a copy of this notice.

_____
Client Name

_____
Printed Name

_____
Signature

_____
Date

Effective date of this notice is March 24, 2025.

Faithful Steps Therapy Solutions of the Big Country
Authorization for Release and/or Disclosure of Health Information

I authorize the disclosure of my personal health information to the persons/entities as described below. I understand this authorization is voluntary, and made to confirm my directions. I understand that once the information is disclosed, it may be re-disclosed and no longer protected by federal privacy regulations. I hereby give permission to Faithful Steps to disclose my personal health information in the manner described herein.

PARTICIPANT'S INFORMATION		
Name:	Last 4 of SSN:	
Birthdate:	Contact Phone Number:	Request Date:
PHI MAY BE DISCLOSED BY:		
Person/Facility:	Phone: Fax #:	
Address:		
PHI MAY BE DISCOLOSED TO		
Person/Facility:	Phone #: Fax: #:	
Address:		

PERSONAL HEALTH INFORMATION TO BE DISCLOSED

1. Specify records to be released and /or disclosed:

□ General Medical Information (from_____to_____)

□ Information Regarding Specific Injury or Treatment (from_____to_____)

□ X-Ray/Laboratory Results of (from_____to_____)

□Mental/Behavioral Health (from_____to_____) Initials of Participant or Representative _____

□Alcohol/Drug (from_____to_____) Initials of Participant or Representative _____

□HIV Test Results (from_____to_____) Initials of Participant or Representative _____

□ Other (specify): _____

2. Your request will be deemed to include any information related to sexually transmitted disease, alcohol or drug use or treatment, or mental health/psychology/psychiatry that may be within your above request, unless you specifically state your objection here:

Right to Revoke: I understand that I may revoke this authorization in writing at any time. I understand my revocation will NOT affect any disclosures that occurred before Faithful Steps received and processed a written notice of revocation. I understand that if I did not specify duration and if I do not revoke it, this authorization will expire one year from the date of signature below. To revoke this authorization, I understand that I must send a written request to Faithful Steps Clinic, ATTN: Privacy Officer, 3444 N 1st St, Ste 508, Abilene, TX 79603, Abilene, Texas 79698.

ACKNOWLEDGEMENT

Please sign and date: I have had full opportunity to read and consider the contents of this authorization, and I confirm that the contents are consistent with my direction to Faithful Steps to release nonpublic personal health information. I understand that Faithful Steps will not condition treatment, payment, enrollment or eligibility for benefits on whether I sign this authorization.

By:_____ _____ _____

Participant's Name (Print) Participant's Signature Date

If you are not the participant, please also complete, sign and date below. Check the box that describes your relationship to the participant. Please attach proof or your relationship tot the participant (e.g. Power of Attorney, legal guardian)

By:_____ _____

Participant's Name (Print) Participant's Signature

□Parent of Minor Child □Legal Guardian □Power of Attorney □Executor □Other _____

Faithful Steps Therapy Solutions of the Big Country
Request for Alternative Means of Communication of Protected Health Information

Use this form to request that you receive communications of protected health information (PHI) by alternative means, or at an alternate location.

Completing this form is voluntary. However, if you would like alternative means of communication of your protected health information, you must provide all of the information requested on this form. Personally identifiable information requested on this form is mandatory in order to process your request and will only be used for this purpose.

INSTRUCTIONS: Mail or hand deliver this completed form to the following address: Faithful Steps Clinic, ATTN: Privacy Officer, 3444 N 1st St, Ste 508, Abilene, TX 79603.

INDIVIDUAL'S INFORMATION		
Name:	Last 4 of SSN:	
Birthdate:	Contact Phone Number:	Request Date:
Current Address (No., street, city, state, zip):		

Please read and complete the following:
At Faithful Steps, we may mail communications containing your PHI to the subscriber (the person receiving the benefits). Communications are addressed to your address as listed in our medical records. We also rely upon telephone information in your medical records when we contact you by telephone. If you believe this method of communication could endanger you, you have the right to request that we:

- Use a reasonable alternate means for communicating your PHI
- Send your PHI to an alternate address
- Contact you at an alternate phone number

Please note that we are not able to accommodate requests for communications to alternate addresses made solely for reasons of convenience.

ALTERNATIVE MEANS OF COMMUNICATION
I request that Faithful Steps communicate with me about my PHI by alternate means, to send such communications to an alternate address, and/or to contact me at an alternate phone number. (Please provide full information regarding the alternate means, address, phone number, etc. that you want us to use.)
I hereby request that any future communications to me from Faithful Steps regarding my health information be directed through alternate methods or means as follows:
❑ Alternative Phone Number: (____)_____
❑ Alternative Mailing Address: (____)_____
❑ Other Alternative Means: _____
_____
State any harm that may occur if this request is denied: _____
_____

ACKNOWLEDGEMENT
Please sign and date:
I have read the above statements and understand that Faithful Steps is not required to agree to every accommodation request, but only required to attempt to accommodate reasonable request when appropriate.

By:_____ _____ _____
Participant's Name (Print) Participant's Signature Date

If you are not the participant, please also complete, sign and date below. Check the box that describes your relationship to the participant. Please attach proof or your relationship to the participant (e.g. Power of Attorney, legal guardian)

By:_____ _____ _____
Participant's Name (Print) Participant's Signature Date

□**Parent of Minor Child** □**Legal Guardian** □**Power of Attorney** □**Executor** □**Other** _____

This Section for Clinic Use Only

❑ **Request APPROVED**
Return a copy of completed form to individual. Send original to Medical Records to make amendment and place in individuals file. Send change to Business Associate(s) as needed.

❑ **Request DENIED**

Reason for Denial: ❑ Too expensive to accommodate request
❑ Administratively impractical to accommodate request
❑ Failure of Participant to specify an alternative accommodation

Send a copy of completed form to individual. Send original to Medical Records to place in individuals Medical Records file.
Date copy sent:_____ Copy sent by (print name: _____

Faithful Steps Therapy Solutions
Request for Accessing/Inspecting/Copying Health Information

As required by the Health Information Portability and Accountability Act of 1996 (HIPAA) you have a right to request the opportunity to inspect and copy health information that pertains to you. Faithful Steps will evaluate your request and will either grant it or explain the reason why the request will not be granted. Faithful Steps may provide you with a summary or explanation of the information in your health plan records instead of access to or copies of your records.

Mail or hand deliver this completed form to: Faithful Steps Clinic, ATTN: Privacy Officer, 3444 N 1st St, Ste 508, Abilene, TX 79603.

INDIVIDUAL'S INFORMATION		
Name:		Last 4 of SSN:
Birthdate:	Contact Phone Number:	Request Date:
Current Address (No., street, city, state, zip):		

REQUEST TO ACCESS/INSPECT/COPY

I am requesting my health information in the following designated record set(s) for the period of time from _____ to _____:

❑ Medical Records ❑ laboratory Reports ❑ Financial Records

❑ Enrollment, payment, claims adjudication information maintained by Faithful Steps

❑ Other agency designated record sets: _____

DELIVERY METHOD

Please check the box indicating how you would like to receive the requested health records.

□ **mail to my current address:** _____
street address city state zip code

□ Pick-up (you will be required to provide photo identification.) Please provide a phone number where we may contact you when copies are ready for pick up. _____

□ Review in person (you will be required to provide photo identification.) Any review of participant records will be conducted in the presence of a clinical staff member. Please provide a phone number where we may contact you to schedule an appointment.
Phone number: _____

ACKNOWLEDGEMENT

Please sign and date: I understand that I may be charged a reasonable cost-based fee for copying my records. Applicable mailing fees also may apply. With certain exceptions, you have the right to inspect or obtain a copy of your health information in a designated record set maintained by Faithful Steps. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative action or proceedings and records that are subject to the Privacy Act, 5U.S.C. 522a.

I further understand there may be circumstances when a licensed health care professional may deny my request for access to my health information; and that I am allowed to request a review by another licensed health care professional.

By:_____ _____ _____
Participant's Signature Participant's Name (Print) Date

If you are not the participant, please complete, sign and date below. Check the box that describes your relationship to the participant. Please attach proof or your relationship to the participant (e.g. Power of Attorney, legal guardian)

By:_____ _____ _____
Participant's Name (Print) Participant's Signature Date

□Parent of Minor Child □Legal Guardian □Power of Attorney □Executor □Other _____

Request Determination on Reverse Side

This Section for Clinic Use Only

Determination:	☐	**REQUEST APPROVED.** Approved date:
Agency Responsibilities:	☐	Determination of method for Participant access. Determination date:
	☐	Notice to Participant of approved access. Sent date:
	☐	Offer Participant summary of information. Sent date:
	☐	Notify Participant of requirements for copies of health information. Sent date:
Determination:	☐	**REQUEST NEEDS FURTHER REVIEW**

Designated Staff Date

Review of Request by Licensed Health Care Professional

Determination:	☐	**REQUEST APPROVED.** Approved date:
Agency Responsibilities:	☐	Determination of method for Participant access. Determination date:
	☐	Notice to Participant of approved access. Sent date:
	☐	Offer Participant summary of information. Sent date:
	☐	Notify Participant of requirements for copies of health information. Sent date:
Determination:	☐	**REQUEST DENIED. Denial date:**
Reason for Denial:	☐	Reference made to another person could endanger that person
	☐	Access could endanger life or physical safety of Participant or other(s)
	☐	Access requested by personal representative and access could cause substantial harm to Participant or other(s)
	☐	Other
Agency Responsibilities:	☐	Written Notice to Participant of basis for denial. Sent date:
	☐	Provide Participant with Opportunity to Request Review by licensed health care professional Sent date:

Licensed Health Care Professional Date

Request Second Review

Determination:	☐	**REQUEST APPROVED**
Agency Responsibilities:	☐	Determination of method for Participant access
	☐	Notice to Participant of approved access
	☐	Offer Participant summary of information
	☐	Notify Participant of requirements for copies of health information
Determination:	☐	**REQUEST DENIED**
Reason for Denial:	☐	Reference made to another person could endanger that person
	☐	Access could endanger life or physical safety of Participant or other(s)
	☐	Access requested by personal representative and access could cause substantial harm to Participant or other(s)
	☐	Other
Agency Responsibilities:	☐	Written Notice to Participant of basis for denial. Sent date:

Licensed Health Care Professional Date

Faithful Steps Therapy Solutions
Request for Amendment of Health Information

As a participant in Faithful Steps's services you have the right to request amendments to your personal health information that are inaccurate or incomplete. If you want to amend your health information, you must complete this form and return it to Faithful Steps Clinic, ATTN: Privacy Officer, 3444 N 1st St, Ste 508, Abilene, TX 79603.

If we deny your request, we will let you know in writing with an explanation of why we are denying it. You have the right to submit a written disagreement to our denial. We will put your statement and requested amendment in to your record. If we continue to disagree with your amendment request, we may put a written rebuttal to your disagreement into your record. If this occurs, we will let you know in writing and send you a copy of our rebuttal.

INDIVIDUAL'S INFORMATION		
Name:	Last 4 of SSN:	
Birthdate:	Contact Phone Number:	Request Date:
Current Address (No., street, city, state, zip):		

REQUESTED AMENDMENT

1. Date(s) of Entry to be amended/corrected: _____

2. Type(s) of Entry to be amended/corrected: _____

3. Please explain how the entry(s) is incorrect or incomplete:

4. What should the entry(s) say in order to be accurate or complete:

5. Would you like this amendment sent to anyone to whom we may have disclosed information to in the past? □NO

□YES If so, please specify the name and address of the organization or individual:

ACKNOWLEDGEMENT
Please sign and date:

By:_____ _____
Participant's Name (Print) Participant's Signature Date

If you are not the participant, please complete, sign and date below. Check the box that describes your relationship to the participant. Please attach proof or your relationship to the participant (e.g. Power of Attorney, legal guardian)

By:_____ _____ _____
Participant's Name (Print) Participant's Signature Date

□Parent of Minor Child □Legal Guardian □Power of Attorney □Executor □Other _____

This Section for Clinic Use Only

Amendment has been: ☐ Accepted ☐ Denied (If denied, check the reason for denial):

- ☐ **PHI (Protected Health Information) was not created by this organization**
- ☐ **PHI is not part of the participant's designed record set**
- ☐ **Federal/State law forbids making corrections to this PHI**
- ☐ **PHI is accurate and**

complete Comments of Faithful Steps

Provider:

~~Amendment has been reviewed by the following Provider(s):~~

_____	_____	_____
Date	**Please Print Name**	**Signature of Provider**
Date	**Please Print Name**	**Signature of Provider**

Notification was sent to the Participant on: _____
Date

Send a copy of completed form to individual. Send original to Medical Records to place in individuals Medical Records file.

Date copy sent:_____Copy sent by (print name: _____

Faithful Steps Therapy Solutions
Request for Restrictions on Use and Disclosure of Health Information

You have the right to request that we restrict how protected health information about you is used or disclosed for treatment, payment, or healthcare operations. We are not required to agree to this request for restriction in whole or in part, but if we do, we are bound by our agreement. Any restriction we accept will not apply when the restricted information is needed to provide you with emergency treatment. This agreement does not apply if release is required by law or if it's against any public health requirements. We further have the right to terminate any agreed upon restriction by informing you of the termination in writing. Any such termination will only apply to information created or received after we have informed you of the termination.

Please complete this form to request a restriction and return it to Faithful Steps Clinic, ATTN: Privacy Officer, 3444 N 1st St, Ste 508, Abilene, TX 79603. We will notify you of our ability to comply with your request by returning a copy of this form to you. You also have the right to request us to terminate a restriction to the extent that such termination applies to information created or received after the date of termination.

INDIVIDUAL'S INFORMATION		
Name:	Last 4 of SSN:	
Birthdate:	Contact Phone Number:	Request Date:
Current Address (No., street, city, state, zip):		

RESTRICTIONS REQUESTED
1. I would like use and disclosure of the following health information to be restricted:
2. I want the information restricted because:
Check the box that tells how you want this information to be restricted and complete the blank:
□ I do not want this information to be given to the following person(s) or agency(s):
□ Other restrictions requested:

ACKNOWLEDGEMENT
Please sign and date:

By:_____ _____ _

_____ Participant's Name (Print)

Participant's Signature Date

If you are not the participant, please complete, sign and date below. Check the box that describes your relationship to the participant. Please attach proof or your relationship to the participant (e.g. Power of Attorney, legal guardian)

By:_____ _____ _____

Participant's Name (Print) Participant's Signature Date

□Parent of Minor Child □Legal Guardian □Power of Attorney □Executor □Other _____

This Section for Clinic Use Only **Request**

has been: ☐ Accepted ☐ Denied (If denied, check the reason for denial):

Comments of Faithful Steps Provider:

Restriction Request has been reviewed by the following Provider(s):

_____	_____	_____
Date	**Please Print Name**	**Signature of Provider**
_____	_____	_____
Date	**Please Print Name**	**Signature of Provider**

Notification was sent to the Participant on: _____
Date

Send a copy of completed form to individual. Send original to Medical Records to place in individuals Medical Records file. Date copy sent:_____Copy sent by (print name: _____

Faithful Steps Therapy Solutions
Accounting of Non-Authorized Use or Disclosure Request Form

The HIPAA Privacy Regulations allow an individual to request an accounting of certain disclosures of his/her Protected Health Information (PHI). Faithful Steps may disclose your PHI for treatment, payment, health care operations, and as required or permitted by the HIPAA Privacy Regulation or other state or federal laws. Our Privacy Notice informs you that these disclosures may occur without your consent at the time they are made.

You can request an accounting of certain disclosures only about yourself, unless you are authorized to obtain information about another individual. Please complete this form to request a disclosure and return it to Faithful Steps Clinic, ATTN: Privacy Officer, 3444 N 1st St, Ste 508, Abilene, TX 79603.

INDIVIDUAL'S INFORMATION		
Name:	Last 4 of SSN:	
Birthdate:	Contact Phone Number:	Request Date:
Current Address (No., street, city, state, zip):		

DISCLOSURE REQUESTED

I request that Faithful Steps provide me with an accounting of any and all applicable "non-authorized" uses and disclosures of my protected health information (PHI) between_____(beginning date) and _____(ending date).

I would like to limit this request for accounting to include disclosures only pertaining to:

_____

I want the accounting of disclosures in the following form: *(check one)*

□ Mail to my current address on file: _____

□ I want to pick up the accounting.
Please call me at the following telephone number when it is ready: _____

I understand that I may be charged for this information if I have previously requested this information within the last 12 months. There will be a fee for any additional accountings within the same 12 month period. I will be informed of the cost for such additional accounting in advance and will be provided with the opportunity to withdraw or modify the request in order to reduce or avoid the fee. I understand that Faithful Steps must give me the accounting of disclosures within 60 days, or must tell me that it needs up to 30 extra days to prepare it.

I understand that Faithful Steps does not have to tell me about the following types of disclosures:

1. Disclosures made prior to April 14, 2003.
2. Disclosures made as part of a limited data set for purposes of research, public health, or health care operations, as permitted by federal law.
3. Disclosures made for purposes of treatment, payment and health care operations.
4. Disclosures made to me or disclosures consented to or authorized by me.
5. Disclosures made to persons involved in my care.
6. Disclosures made for national security or intelligence purposes.
7. Disclosures made to correctional institutions or law enforcement officials, under certain circumstances.
8. Disclosures made incident to a use or disclosure otherwise permitted or required by law.

I also understand that my right to an accounting of some or all disclosures may be suspended by the government under limited circumstances.

ACKNOWLEDGEMENT
Please sign and date:

By:_____ _____ _

_____ Participant's Name (Print)
Participant's Signature Date

If you are not the participant, please complete, sign and date below. Check the box that describes your relationship to the participant. Please attach proof or your relationship to the participant (e.g. Power of Attorney, legal guardian)

By:_____ _____ _____
Participant's Name (Print) Participant's Signature Date

□Parent of Minor Child □Legal Guardian □Power of Attorney □Executor □Other _____

Request Determination on Reverse Side

This Section for Center Use Only

Privacy Officer Action/Comments:
Action must be taken within 60 days of the receipt of the request
Request has been: ◆ Accepted ◆ Denied (If denied, please

explain): Comments of HLC Provider:

Disclosure Request has been reviewed by the following Provider(s):

Date	**Please Print Name**	**Signature of Provider**
Date	**Please Print Name**	**Signature of Provider**

Notification was sent to the Participant on:

Date

Send a copy of completed form to individual. Send original to Medical Records to place in individuals Medical Records file. Date copy sent: Copy sent by (print name:

Faithful Steps Therapy Solutions of the Big Country

BUSINESS ASSOCIATE AGREEMENT

This Agreement ("Agreement") is made and entered into this day of Month:_____, Year by and between Faithful Steps ("Covered Entity"), whose business address is 3444 N 1st St, Ste 508, Abilene, TX 79603 and Business Name:_____("Business Associate"), Type of Entity: _____, whose business address is Address of Business Associate:_____.

1. **Definitions.** Terms used, but not otherwise defined in this Agreement, shall have the same meaning as those terms in the Privacy Rule and the Security Rule.

   a. **Business Associate**. "Business Associate" shall mean [Name of Business Associate].

   b. **Covered Entity**. "Covered Entity" shall mean Faithful Steps.

   c. **Individual**. "Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

   d. **Privacy Rule**. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

   e. **Protected Health Information**. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

   f. **Required By Law**. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR §164.103.

   g. **Secretary**. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

   h. **Security Rule**. "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. parts §160 and §164, subparts A and C.

2. **Obligations and Activities of Business Associate.**

   a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required by Law.

   b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement. Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any electronic Protected Health Information that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity, as provided for in the Security Rule.

   c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

   d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware. Business Associate also

agrees to report to Covered Entity any security incident, including all data breaches whether internal or external, related to Protected Health Information of which Business Associate becomes aware.

e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f. Business Associate agrees to provide access, at the request of Covered Entity and during normal business hours, to Protected Health Information in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR §164.524, provided that Covered Entity delivers to Business Associate a written notice at least five (5) business days in advance of requesting such access. This provision does not apply if Business Associate and its employees, subcontractors and agents have no Protected Health Information in a Designated Record Set of Covered Entity.

g. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR §164.526, at the request of Covered Entity or an Individual. This provision does not apply if Business Associate and its employees, subcontractors and agents have no Protected Health Information from a Designated Record Set of Covered Entity.

h. Unless otherwise protected or prohibited from discovery or disclosure by law, Business Associate agrees to make internal practices, books, and records, including policies and procedures, relating to the use or disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, available to the Covered Entity or to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule or Security Rule. Business Associate shall have a reasonable time within which to comply with requests for such access and in no case shall access be required in less than five (5) business days after Business Associate's receipt of such request, unless otherwise designated by the Secretary.

i. Business Associate agrees to maintain necessary and sufficient documentation of disclosures of Protected Health Information as would be required for Covered Entity to respond to a request by an Individual for an accounting of such disclosures, in accordance with 45 CFR §164.528.

j. On request of Covered Entity, Business Associate agrees to provide to Covered Entity documentation made in accordance with this Agreement to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R.§164.528. Business Associate shall have a reasonable time within which to comply with such a request from Covered Entity and in no case shall Business Associate be required to provide such documentation in less than five (5) business days after Business Associate's receipt of such request.

k. Except as provided for in this Agreement, in the event Business Associate receives an access, amendment, accounting of disclosure, or other similar request directly from an Individual, Business Associate will redirect the Individual to the Covered Entity.

3. Permitted Uses and Disclosures by Business Associate.

a. Except as otherwise limited by this Agreement, Business Associate may make any uses and disclosures of Protected Health Information necessary to perform its services to Covered Entity and otherwise meet its obligations under this Agreement, if such use or disclosure would not violate the Privacy Rule if done by Covered Entity. All other uses or disclosures by Business Associate not authorized by this Agreement or by specific instruction of Covered Entity are prohibited.

b. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

c. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

d. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B).

e. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).

4. Obligations of Covered Entity.

a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

5. Term and Termination.

a. Term. The Term of this Agreement shall be effective as of [Effective Date] , and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Agreement.

b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall give Business Associate written notice of such breach and provide reasonable opportunity for Business Associate to cure the breach or end the violation. Covered Entity may terminate this Agreement, and Business Associate agrees to such termination, if Business Associate has breached a material term of this Agreement and does not cure the breach or cure is not possible. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

c. Effect of Termination.

1. Except as provided in paragraph (2) of this section, upon termination of this Agreement for any reason, Business Associate shall return or destroy all Protected Health Information received from or created or received by Business Associate on behalf of, Covered Entity. This provision shall apply to Protected Health Information that is in the

possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity, within ten (10) business days, notification of the conditions that make return or destruction infeasible. Upon such determination, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6. Miscellaneous.

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule or Security Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

c. Survival. The respective rights and obligations of Business Associate under Section 5(c) of this Agreement shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule or the Security Rule.

7. **Counterparts.** This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which together shall constitute one original Agreement. Facsimile signatures shall be accepted and enforceable in lieu of original signatures.

APPROVED AND ACCEPTED BY:

Business Associate Print Name & Title	Signature	Date
Hardin-Simmons University	Signature	Date

Faithful Steps Therapy Solutions
INCIDENT REPORT

Date of Incident:_____ Time of Incident:_____am/pm

Faithful Steps Location: _____

Person(s) Involved Name:_____If Participant, Last 4 of SSN:_____
(Circle one) Participant Staff Volunteer Contractor Other_____

Witness(es)_____

NATURE OF INCIDENT (check all that apply):

- o HIPAA Violation/Breach of Confidentiality
- o Complaint/Grievance
- o Equipment / Supplies
- o Facility Safety and Security
- o Inappropriate Behavior
- o Injury (specify type)_____
- o Medication error
- o Medical Emergency
- o Property Damage/TheftOther _____

Notified: Police Fire Ambulance

DETAILS OF INCIDENT (include all known facts, persons involved, statements, cause, witnesses, time, location)

RESOLUTION (if applicable)

REPORTING

Note: Incidents must be reported within 24 hours of occurrence. A copy of this form must be given to department supervisor or Privacy Officer

---

Incident Reported to: _____ Title:_____

_____ Date:

_____

Report completed by:_____Title:_____ Date:_____

Contact Phone number:_____Dept.: _____

OFFICIAL REVIEW

Incident reviewed by:

- o Privacy Officer
- o Incident Response Team
- o Other _____

If applicable, Severity of HIPAA Privacy Incident:

Severe	Press may be involved. Affects participant and/or public, business associates, and/or state and/or local government.
□ Moderate	Press involvement unlikely. Affects participant and/or business associates.
□ Low	No affect outside of Clinic. Clinic able to resolve

COMMENTS BY REVIEWER(S):

RESOLUTION/CORRECTIVE ACTION:

Staff Training Needed	Procedures to be Reviewed	Employee Sanctions
Inform Participant	Record disclosure in accounting of disclosures log with Privacy Off.	Other

o No further action required, ok to file

Signature:_____ Title:_____ Date: _____

THIS IS A CONFIDENTIAL REPORT FOR OFFICIAL USE ONLY. DO NOT FILE IN PARTICIPANT'S RECORD.

Faithful Steps Therapy Solutions
COMPLAINT REPORT

Today's Date: _____

All information can be submitted anonymously, any identifying information is not required.

Name (Optional):	Last 4 of SSN:
Address:	Phone Number:

If you are filing a complaint on someone's behalf, provide the name and address of the person on whose behalf you are filing.

Name: _____

Address: _____

Please describe in detail the nature of your complaint, including the date or dates of the incident(s), and the name or names of any Faithful Steps staff member and other witnesses (attach additional sheets if necessary):

_____

_____

_____

_____

_____ _____

Participant or Legal Representatives' Signature Date

_____

Relationship (if not Participant)

Send to: Faithful Steps Therapy Solutions
ATTN: Privacy Officer
3444 N 1st St., Ste 508, Abilene, TX 79603
Fax: 325-244-1125

For Internal Use Only:

Manager's acknowledgement of receipt Print Name: Date received: / /

Process of Investigation:

Formal Action Taken/Resolution:

COO or Privacy Office Comments:

COO or Privacy Officer Signature If COO place in QA File, If for Privacy Officer place in HIPAA Log Binder

FEDERAL PRIVACY LAWS

Federal

HIPAA Privacy Rules:
The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without participant authorization. The Rule also gives participants' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

HIPAA Security Rules:
The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

42 CFR Part 2 – Confidentiality of Alcohol and Drug Abuse Participant Records:
42 CFR Part 2 applies to AOD programs that are federally conducted, regulated or assisted in any way, directly or indirectly. Regulations apply to recipients of AOD and their participant identifiable information and prohibit most disclosures of information without participant consent.
http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl

Genetic Information Nondiscrimination Act (**GINA**)**:**
Under Title II of GINA, it is illegal to discriminate against employees or applicants because of genetic information. Title II of GINA prohibits the use of genetic information in making employment decisions, restricts employers and other entities covered by Title II (employment agencies, labor organizations and joint labor-management training and apprenticeship programs - referred to as "covered entities") from requesting, requiring or purchasing genetic information, and strictly limits the disclosure of genetic information.
http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/html/PLAW-110publ233.htm