PURPOSE

Signify Health, LLC and its subsidiaries (collectively “Company”), is committed to ensuring the confidentiality, integrity, availability, and security of all Protected Health Information (“PHI”) it creates, receives, maintains, and/or transmits in compliance with the requirements of the Health Insurance Portability Accountability Act of 1996, as amended, with its implementing regulations which established, without limitation, the Privacy Rule, the Security Rule, the HITECH Act, and the Breach Notification Rule (collectively “HIPAA”). Company may be referred to herein as “we” or “our.”

POLICY

All Workforce members are responsible for safeguarding PHI in accordance with HIPAA and Company’s policies and procedures. This HIPAA Privacy Program Policy (“Policy”) sets forth the appropriate development, implementation, and oversight of Company’s efforts toward compliance with HIPAA. This Policy covers, without limitation, the designation of Privacy and Security Officers, required Workforce training, the process for investigating and reporting potential HIPAA violations, and HIPAA-compliant processes for Individual requests concerning records. Additional information security rules and procedures are set forth in Company’s Information Security Policy.

DEFINITIONS/ACRONYMS

“BAA” means Business Associate Agreement.

“Breach” shall be defined herein as defined in 45 CFR §164.402. In general, Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI.
“Breach Notification Rule” shall be defined herein as defined by 45 CFR §§ 164.400-414. In general, the rule requires HIPAA Covered Entities and their Business Associates to provide notification following a breach of unsecured PHI.

“Business Associate” shall be defined as provided in 45 CFR §160.103. A Business Associate is a person or organization, other than a member of a Covered Entity’s Workforce, that performs certain functions or activities on behalf of, or to, a Covered Entity that involves the access, use, or disclosure of Individually Identifiable Health Information. A Covered Entity may be a Business Associate of another Covered Entity. Company may be, in certain circumstances, a Business Associate with respect to our health plan clients.

“Covered Entity” shall have the same meaning as the term “Covered Entity” at 45 CFR §160.103.

“Disclosure” means the release, transfer, provision of access to, or divulging in any manner of information outside Company.

“Electronic PHI” or “ePHI” shall mean any PHI maintained in or transmitted by electronic media as defined in 45 CFR § 160.103. Electronic PHI or “ePHI” includes any medium used to store, access, transmit or receive PHI electronically. Examples include, but are not limited to:

- Personal computers with their internal hard drives used at work, home or traveling;
- External portable hard drives;
- Magnetic tape or disks;
- Removable storage devices such as USB memory sticks/keys, CDs, DVDs, and floppy diskettes;
- PDAs, smartphones, iPhones, iPads, computers, tablets;
- Electronic transmission includes data exchange (e.g., email or file transfer) via wireless, Ethernet, modem, DSL or cable network connections; and
- Internet and cloud based devices.

As technology progresses, any new devices for accessing, transmitting, or receiving ePHI electronically will be covered by the HIPAA Security Rule.

“Health Care Operations” shall have the meaning given to that term at 45 CFR § 164.501.

“HHS” shall mean the U.S. Department of Health and Human Services.

“HIPAA Regulations” shall be defined herein as the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including but not limited to, 45 CFR §§ 160 and 164, as are currently in effect or as later amended.

“HITECH” shall be defined herein as the Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111–5.
“Hotline” means Company’s anonymous compliance telephone hotline at: **1+(844) 232-8709**.

“**Individual**” means the person who is the subject of PHI and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

"**Individually Identifiable Health Information**" is information, including demographic data, that relates to:

- the Individual’s past, present or future physical or mental health or condition,
- the provision of health care to the Individual, or
- the past, present, or future payment for the provision of health care to the Individual, and that identifies the Individual or for which there is a reasonable basis to believe it can be used to identify the Individual.

Individually identifiable health information includes many common identifiers, including, but not limited to, any of the following identifiers for an Individual or for the Individual’s employer or family member, or if a Workforce member is aware that the information could be used, either alone or in combination with other information, to identify an Individual:

- Name;
- Address (all geographical subdivisions smaller than state, including street address, city, county, zip code);
- All elements (except years) of dates related to an Individual (including birth date, admission date, discharge date, date of death and exact age if over 89);
- Telephone number;
- Fax number;
- Email address;
- Social Security Number;
- Medical record number;
- Health plan beneficiary number;
- Account number;
- Certificate/license number;
- Any vehicle or other device serial number;
- Device identifiers or serial numbers;
- Web URL;
- Internet Protocol (IP) address number;
- Finger or voice prints;
- Photographic images; and
- Any other characteristic that could uniquely identify the Individual.

“**Minimum Necessary Standard**” or “Minimum Necessary” means the HIPAA Privacy standard established at 45 CFR §164.502(b) requiring that any authorized access, use, disclosure, or request of PHI be limited to the minimum necessary to accomplish the intended purpose within one’s job duties. The minimum amount of information necessary is dictated, in part, by Company’s Technology Department policy(s) or protocol setting the least privileged role within a Workforce member’s
assignment. Simply put, access/use/disclosure of PHI shall be the least amount required to do your job.

“Personal Representative” means a person authorized by law to act on behalf of an Individual to make healthcare decisions and/or review the Individual’s PHI. Duly authorized Personal Representatives have the same rights as the Individual under HIPAA.

“Privacy Officer” is Company’s designated HIPAA Privacy Officer and Contact Person at 4055 Valley View Lane, Suite 400, Dallas, TX 75244, (469) 466-7035 Phone, 1+(214) 279-8063 eFax. Privacy Officer is responsible for the development, implementation and enforcement of Company’s health related privacy policies and procedures. Privacy Officer is the contact person responsible for responding to requests for further information and receiving complaints regarding Company’s health related privacy policies and procedures.

“Privacy Rule” shall be defined herein as the standards of privacy of Individually Identifiable Health Information at 45 CFR §§160 and 164, Subparts A and E.

"Protected Health Information" or "PHI" as defined by 45 CFR §160.103, means Individually Identifiable Health Information held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic, paper, or oral. PHI does not include certain employment or education records, or Individually Identifiable Health Information regarding an Individual who has been deceased more than 50 years.

“Security Officer” is Company’s Information Security Officer at 4055 Valley View Lane, Suite 400, Dallas, TX 75244, (469) 466-7710 Phone. Security Officer is responsible for the development and implementation of policies and procedures to ensure the integrity of Company’s electronic PHI.

“Security Rule” shall be defined herein as the standards of security requirements of the HIPAA Regulations at 45 CFR §§302 through §164.31.

“Unsecured Protected Health Information or PHI” shall mean any PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized Individuals through the use of a technology or methodology specified by the Secretary in the guidance issued pursuant to §13402(h) (42 U.S.C. § 17932(h)) of the HITECH Act.

“Workforce” as defined by 45 CFR §160.103, means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate. Therefore, Company’s Workforce includes all Individuals who act on our behalf, perform work for us, and act at our direction, facilitating our normal business operations. Persons who fall within this category include employees, volunteers, trainees, independent contractors, clinicians, and leased or temporary workers.

Note: Capitalized terms used, but not otherwise defined, in this HIPAA Privacy Program Policy shall have the same meaning as those terms in HIPAA, HIPAA Regulations and HITECH.
HIPAA PROGRAM POLICY CONTENTS

I. Overview & General Rules
II. Privacy of Individually Identifiable Health Information
III. Amendment of Protected Health Information
IV. Accounting of Disclosures
V. Members of the Workforce – Training & Conduct
VI. Creating and Maintaining Privacy Compliance Records
VII. Requests for Access to Records
VIII. Resolution of Objections and Complaints
IX. Breaches
X. Reporting/Questions/Enforcement

PROCEDURE

I. Overview & General Rules

A. HIPAA Overview

HIPAA applies to persons and entities engaged in the handling of health information. HIPAA also applies to the Business Associates of Covered Entities, either directly or through a mandatory contractual agreement, often times called a Business Associate Agreement or BAA. Generally, HIPAA:

- Gives Individuals control over the use of their health information;
- Defines boundaries for the access/use/disclosure of health information;
- Establishes national-level standards of compliance;
- Helps to limit the use of PHI and minimizes chances of its inappropriate disclosure;
- Strictly investigates compliance-related issues and holds violators accountable with civil or criminal penalties for violating the privacy of an Individual’s PHI; and
- Supports the cause of disclosing PHI without Individual consent for Individual healthcare needs, public benefit, and national interests.

B. HIPAA Standards

HIPAA imposes the following standards for the purpose of standardizing and protecting the access, use, disclosure, and exchange of health information:

- Privacy standards, developed by HHS, that address the use and disclosure of health information, patient consent and authorization for the use of information, patient rights to review their health information, request edits and demand an accounting of disclosures of health information.
- Security standards for health information including administrative, technical, and physical safeguards to ensure the integrity and confidentiality of health information and to protect against security Breaches and unauthorized use or disclosure of health information.
• Standards for the transfer of information among health plans needed, for example, for the coordination of benefits, sequential processing of claims.
• Standards to enable electronic interchange. HIPAA calls for the adoption of standards for certain transactions and data elements, such as health claim status, eligibility for a health plan, health plan enrollment/disenrollment.
• Standards for code sets for the data elements for the transactions covered above.
• Standards for unique health identifiers for Individuals, employers, health plans, and health care providers.
• Standards for electronic signatures.
• Requirements related to notifying patients and DHHS in the event of a Breach of PHI.

C. Safeguarding Information – Minimum Necessary
You are only permitted to access, use, or disclose the Minimum Necessary PHI and other confidential information required to perform your specific job functions. If you see or hear information in the course of doing your job that you do not need to know, remember that this information is confidential. You are not permitted to repeat it or share it with others – even friends, family, or other employees who do not have a need to know it.

All Company employees play an important role in safeguarding sensitive information. You are obligated to maintain privacy and safeguard PHI. There are many ways that confidential information can be inappropriately accessed, used, or disclosed. These may include computer viruses, theft of computer equipment, records, and/or information or unauthorized disclosure of information. Report any such incidents to your supervisor and the Privacy Officer immediately.

1. Photocopiers / Scanners
   a) When making copies or scanning confidential information, do not leave the copier until your job is complete.
   b) Be sure to remove all papers containing confidential information.
   c) Check all areas of the photocopier, including the output tray, the input feeder, and the top of the glass surface.
   d) Do not allow others to see the information you are copying.
   e) Securely destroy (per the Disposal of PHI and other Confidential Information provision of this Policy) or return any confidential information that has been left on a photocopier to the owner.

2. Fax Machines
   a) The faxing of PHI should be performed only when absolutely necessary; other, more secure ways of sending information should be considered (i.e., SFTP site).
   b) If you must fax, you are required to only use Company’s secure faxing system approved by Technology and include Company’s standard fax cover sheet that contains a confidentiality disclaimer and instructions on what to do if accidently received.
   c) Be sure to confirm the fax and telephone numbers of the fax recipient(s).
d) Prior to faxing confidential information, alert the person you are faxing so that he/she can retrieve the fax from the machine immediately.

e) Follow up with the person to verify that he/she received the fax.

f) Securely destroy (per the Disposal of PHI and other Confidential Information provision of this Policy) confidential information that has been received in error and advise the sender of the error.

g) Immediately notify your supervisor and the Privacy Officer to report inadvertent faxing to the wrong person.

D. **Disposal of PHI and other Confidential Information**

Never discard paper, computer disks, or other portable media that contain member information in a wastebasket. Confidential information, including PHI, must be discarded utilizing a shredder or a receptacle provided by Company’s shredding vendor. HIPAA compliant methods for destruction/disposal of PHI include, without limitation:

**Paper:** Shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

**Electronic media:** Destruction must be in accordance with HIPAA and the National Institute of Standards and Technology ("NIST") requirements implemented by Company’s Technology Department and reflected in its policies. Examples include, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding). Do not destroy electronic media yourself. Instead, submit all electronic media, including without limitation, flash drives, laptops, disks, and iPads, to Technology to dispose or destroy PHI.

If you are unsure how to dispose of PHI or other confidential information, contact your supervisor, the Privacy Officer, or the Security Officer.

E. **Reporting HIPAA Violations**

It is every employee’s responsibility to be alert to unethical behavior or possible violations of Company HIPAA policies. If you witness or suspect inappropriate access, use, or disclosure of PHI, immediately notify your supervisor, the Privacy Officer, the Security Officer, or Company’s anonymous compliance telephone Hotline at: **1 + (844) 232-8709.**

If it is determined that there was a Breach, Company will report in accordance with HIPAA and the terms of any applicable BAA. There are a variety of exceptions where an incident does not constitute a reportable Breach, including situations where it is unlikely that the information could be misused – this decision may only be made by the Privacy Officer following an investigation.

II. PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION
Company protects the confidentiality of PHI as required by law.

A. **Our Duties & Privacy Notice**
   When Company is performing as a Covered Entity, we are required by law to maintain the privacy of Individuals’ Protected Health Information and to provide them with notice of our legal duties and privacy practices with respect to PHI. We are required to abide by the terms of this notice but reserve the right to change the terms of the notice and to make the new notice provisions effective for all PHI we maintain. If we change the terms of notice, we will provide applicable Individuals with a copy of the revised notice by hand-delivery or mail.

B. **Protected Information**
   In order to conduct operations, our designated agents or we, collect, create and/or use different types of information. This may include information about an Individual such as his or her name, address, age, health status, and information about dependents. Some of this information may qualify as Protected Health Information. Our use or disclosure of PHI may be restricted or limited by law.

C. **Permitted Uses and Disclosures of Protected Health Information**
   1. **For Payment.** Our designated agents or we may use and disclose information about an Individual in obtaining or making payment to others for services we provide to Individuals. This may include such functions as reimbursing health care providers for services, determining eligibility or coverage of an Individual, performing coordination of benefits, health care data processing including claims management, collection activities, obtaining payments under a reinsurance contract, and/or medical necessity reviews.

   2. **For Health Care Operations.** Our designated agents or we may use and disclose information about an Individual for health care operations. This may include information about an Individual needed to review the quality of care and services he or she receives, to provide case management or care coordination services, provide treatment alternatives or other health-related benefits and services, and/or to perform audits, ratings, and forecasts (as limited by HIPAA standards).

   3. **For Treatment.** Our designated agents or we may use and disclose information about an Individual for treatment purposes. This may include information needed for the provision, coordination, or management of health care and related services.

   4. **As Permitted or Required by Law.** Information about an Individual may be used or disclosed to a Covered Entity that provides services to said Individual and with which Company has a BAA for services concerning the same Individual, regulatory agencies, for administrative or judicial proceedings, for health oversight activities, to law enforcement officials when required to comply with a court order or subpoena, and/or as authorized by and to the extent necessary to comply with workers’
compensation laws.

5. **Public Health Activities.** Information about an Individual may be used or disclosed to a public health authority for the purposes of preventing and controlling disease, injury or disability, reporting child abuse or neglect, and/or to assist the Food and Drug Administration in tracking products and defects/problems as well as enabling product recalls and conducting post marketing activities. Information about an Individual may also be used or disclosed if we reasonably believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

6. **Abuse, Neglect or Domestic Violence.** To the extent required or authorized by law, or with the Individual’s consent, protected information about him or her may be disclosed to an appropriate government authority if we reasonably believe the Individual is the victim of abuse, neglect, or domestic violence.

7. **In the Event of Death.** In the event of an Individual’s death, our designated agents or we may disclose the Individual’s protected information to coroners, medical examiners and/or funeral directors as necessary to carry out their duties.

8. **Organ Transplant.** Our agents or we may use or disclose an Individual’s protected information to organ procurement organizations or related entities for the purpose of facilitating organ, eye or tissue donation and transplantation.

9. **Research Purposes.** Our agents or we may use or disclose an Individual’s protected information for research provided we first obtain an authorization or waiver from the Individual and representations from the researcher limiting the uses and protecting the privacy of the Individual’s information. Aggregate data may be used for said purposes assuming that all outputs are cleansed of any Individual protected information.

10. **Correctional Institutions.** Our agents or we may use or disclose an Individual’s protected information to a correctional/custodial institution or appropriate law enforcement official if the Individual is an inmate and the disclosure is necessary for his or her health care and the health and safety of the Individual, other inmates, officers or institution employees.

11. **Minimum Necessary Required.** When accessing, using, disclosing, or requesting an Individual’s information, we are normally required to make reasonable efforts to limit PHI to the Minimum Necessary to accomplish the intended purpose of the use, disclosure or request. This limitation does not apply in situations involving disclosures to the Individual or made pursuant to his or her authorization, to a health care provider for treatment, to the Secretary of HHS for HIPAA compliance and enforcement purposes, or as otherwise required by law.
12. **Authorization.** Other uses and disclosures of PHI will be made only with the Individual's written permission, unless otherwise permitted or required by law. An Individual may revoke in writing, any such authorization unless we have taken action in reliance on the authorization or it was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy.

13. **Disease Exposure.** Our designated agents or we may disclose an Individual's information to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, as necessary in the conduct of a public health intervention or investigation.

14. **Informational Contact.** We may contact Individuals to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the Individuals.

D. **Availability of Notice on Our Website**  
We will prominently post our privacy notice on our website and make it available electronically through our website.

E. **Rights of Individuals – Access/Copy/Amend/Request to Restrict/Accounting of Disclosures**  
Individuals have the right to:

- Send us a written request to see or get a copy of the PHI that we have about them.
- Send us a written request to amend their personal information that they believe is incomplete or inaccurate. The request must provide a reason to support the requested amendment.
- Request, in writing, additional restrictions on uses or disclosures of their Protected Health Information to carry out treatment, payment, or health care operations. However, we are not required to agree to these requests.
- Receive an accounting of our disclosures of their Protected Health Information in writing, except when those disclosures are made for treatment, payment or health care operations, or when the law otherwise restricts the accounting.
- Receive a paper copy of notice of the rights listed in this section upon request.
- Individuals cannot be forced to waive their rights established by the privacy regulations.
- Request that we communicate with Individuals about medical matters using reasonable alternative means or at an alternative address.

F. **Complaints**  
Individuals who believe their HIPAA privacy rights have been violated have the right to file a complaint with either the Secretary of the U.S. Department of Health and Human Services, 200 Independence Ave., S.W., Washington, D.C. 20201, or Company’s Privacy Officer at 4055 Valley View Lane, Suite 400, Dallas, TX 75244. The complaint should be in writing, either on paper or in electronic format, and generally describe the
acts or omissions believed to be in violation of the Individual’s rights. Individuals will not be retaliated against for filing a complaint.

G. **Further Information**  
Individuals who need further information should contact Company’s Privacy Officer.

### III. AMENDMENT OF PROTECTED HEALTH INFORMATION

A. **Right to Request Amendment**  
Individuals have the right to request that we amend Protected Health Information or records about them that are in our possession.

B. **Form of Request**  
All requests for amendment must be submitted in writing, describe the specific amendment sought, and provide a general description of the reasons for the requested amendment.

C. **Time Frame for Responding to a Request for Amendment**  
Once we receive the written request to amend information, we will attempt to act on it within sixty (60) days. If we cannot meet the 60-day deadline, we may extend the period once for up to an additional thirty (30) days. In that event, we will give the Individual advance (before the expiration of the original 60 days) written notice of the extension and provide a statement of the reason(s) for delay.

D. **Granting the Requested Amendment**

1. **Notice to the Individual.** If we grant the requested amendment, in whole or in part, we will notify the Individual of our decision and request the following from them:
   a) The identification of persons who have received Protected Health Information about them and who need notice of the amendment; and
   b) The Individual's agreement to allow us to provide notice of the amendment to (1) the persons the Individual identifies and (2) persons and entities we know who have the information that is the subject of the amendment and that may have relied, or could potentially rely, on the information to their detriment.
   c) In order to notify necessary third parties, we are required to take reasonable steps to obtain this information from the Individual. If the Individual refuses or fails to provide the information, we will document all efforts we have undertaken to obtain the information. The Individual’s failure or refusal to cooperate does not alter our obligation to make the appropriate amendment.

2. **Amending the Information.** Once we have obtained the information concerning parties to be notified as described above, and the Individual's agreement, we will make the appropriate amendment by identifying the records that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
3. **Notice to 3rd Parties.** We will provide written notice of the amendment to any person (or entity), including a Business Associate, who:
   a) Has received Protected Health Information about the Individual in the past and needs notice of amendment, and/or
   b) Possesses the Protected Health Information that is the subject of the amendment and may have relied, or could potentially rely, on the information to the Individual’s detriment.

E. **Request Granted only in Part**
In the event that only part of the requested amendment is granted, we will follow the procedures set forth below with regard to the denial of the remaining portion of the request.

F. **Denying the Requested Amendment**
   1. **Grounds for Denial.** We may deny an Individual’s request for an amendment if we determine that the Protected Health Information or record that is the subject of the request:
      • Was not created by us (unless the Individual provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment);
      • Is not part of our records;
      • Is not available for the Individual’s access under federal law and/or our policy regarding rights to access; or
      • Is accurate and complete.

   2. **Notice of Denial.** If we deny a request for amendment, in whole or in part, we will notify the requesting Individual of our decision in writing and include a plain language description of the reason(s) for our denial, and explanation of the Individual’s rights, as set forth below, in response to our denial, and a description of how the Individual may lodge a complaint about the decision.

   3. **Individual’s Right to Submit a Statement of Disagreement.** If we deny a request for amendment, in whole or in part, the Individual has the right to submit a written statement disagreeing with our denial and the reason(s) for the disagreement. The statement of disagreement should not exceed 1000 words and must be submitted to Company’s Privacy Officer at 4055 Valley View Lane, Suite 400, Dallas, TX 75244, 1+(214) 279-8063 eFax, within twenty-one (21) days of the Individual's receipt of the notice of denial. The Individual will waive his or her right to file a statement of disagreement if he or she fails to comply with these requirements. We may prepare a written rebuttal to the Individual’s statement of disagreement. If we do so, we will provide a copy to the Individual.

   4. **Other Rights.** If the Individual does not submit a statement of disagreement, he or she may request that we provide copies of the request for amendment and the denial notice with any future disclosures of the Protected Health Information that is the
subject of the amendment.

5. **Record of Denial.** If we deny a request for an amendment, in whole or in part, we will maintain record that identifies the record or information that is the subject of the disputed request for amendment, and append to the records, or otherwise link, the Individual's request for amendment, our denial, and, if applicable, the Individual's statement of disagreement and our rebuttal, if any.

6. **Future Disclosures – Statement of Disagreement on File.** If the Individual has submitted a statement of disagreement, we will include the information identified in the *Record of Denial* section, above, or an accurate summary of such information, with any subsequent disclosure of the information to which the disagreement relates.

7. **Future Disclosures – No Statement of Disagreement Submitted.** If the Individual does not submit a timely statement of disagreement, we will include the request for amendment and our denial, or an accurate summary of such information, with any subsequent disclosure of the information to which the disagreement relates.

8. **Future Disclosures – Situations Where Additional Material Cannot Be Provided.** If we make a subsequent disclosure using a standard transaction that does not permit additional material to be included with the disclosure, we will separately submit any required material to the recipient.

F. **Our Receipt of Amendment by another Entity**
   If we receive notice from another entity that the entity has amended an Individual’s Protected Health Information, we will amend any applicable information in our records.

G. **Complaints**
   Individuals who believe their HIPAA privacy rights have been violated have the right to file a complaint with either the Secretary of the U.S. Department of Health and Human Services, 200 Independence Ave., S.W., Washington, D.C. 20201, or Company’s Privacy Officer at 4055 Valley View Lane, Suite 400, Dallas, TX 75244, 1+(214) 279-8063 eFax. The complaint should be in writing, either on paper in electronic format, and generally describe the acts or omissions believed to be in violation of the Individual’s rights. Individuals will not be retaliated against for filing a complaint.

IV. **ACCOUNTING OF DISCLOSURES**

A. **Right to an Accounting**
   Individuals have a right, subject to certain limitations, to receive an accounting of our disclosures of their Protected Health Information.

B. **Covered Time Period**
The right to an accounting of disclosures extends back six (6) years prior to the Individual’s request for an accounting. The Individual may limit their request to a time period less than six (6) years.

C. **Limitations on Right to Accounting**
Individuals do not have a right to an accounting of the disclosures we have made for the following reasons:

- To carry out treatment, payment and health care operations, in accordance with our privacy policies;
- To the Individual in response to their request for such a disclosure;
- Incident to a use or disclosure otherwise permitted or required by law, including secondary uses or disclosures that cannot reasonably be prevented, are limited in nature, and that occur as a result of another use or disclosure that is permitted by law;
- Pursuant to a valid authorization, signed by the Individual, that allows us to use or disclose their Protected Health Information;
- For our facility directory, to persons involved in the Individual’s care, or for notification purposes in emergency or exigent circumstances as allowed under federal law;
- To correctional institutions or law enforcement officials in certain limited situation;
- As part of a limited data set that excluded all references to personal identification information; or
- That occurred prior to the date on which we became subject to the Department of Health and Human Services' HIPAA Privacy Rule.

D. **Temporary Suspension of Right to Accounting**
We may be required to temporarily suspend an Individual’s right to an accounting of disclosures to a health oversight agency or law enforcement official for a certain period of time if we are notified by a health oversight agency or law enforcement official/agency that such an accounting to the Individual would be reasonably likely to impede the agency’s activities. If possible, we should obtain from the requesting agency/official a written statement detailing the notice of the length of time for which suspension is required. If the statement is made orally, we are still required to suspend the right, but also must:

- Document the statement, including the identity of the agency/official making the statement; and
- Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless the agency/official provides a written statement during that time period.

E. **Content of Accounting**
The accounting of our disclosures or an Individual’s Protected Health Information will include the following information:
• An itemized list of each disclosure of Protected Health Information that occurred during the relevant time period (unless the disclosure was made pursuant to one of the exempt categories set forth above);
• The date of each disclosure;
• The name and address (if known) of the entity or person who received the information;
• A brief description of the information disclosed; and
• A brief statement of the purpose of the disclosure.

F. **Abbreviated Accounting**
We may provide an abbreviated, but meaningful, summary of the disclosures if we have made multiple disclosures to the same person or entity for a single purpose. The summary must include the following information:
• The same detailed information required for an accounting of a normal disclosure, but only with respect to the first disclosure during the accounting period;
• The frequency, periodicity, or number of the disclosures made during the accounting period; and
• The date of the last such disclosure during the accounting period.

We may also provide an abbreviated, but meaningful summary, if we have made disclosures for a particular research purpose for fifty (50) or more Individuals. The summary must include the following information:
• The name of the protocol or other research activity;
• A plain language description of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
• A brief description of the type of Protected Health Information that was disclosed;
• The date or period of time during which such disclosures occurred, including the date of the last such disclosure during the accounting period;
• The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
• A statement that the Protected Health Information of the Individual may or may not have been disclosed for a particular protocol or other research activity.

If we provide an accounting for research disclosures, and it is reasonably likely that the Protected Health Information of the Individual was disclosed for such research protocol or activity, we shall, at the request of the Individual, assist in contacting the entity that sponsored the research and the researcher.

G. **Time Frame**
Once we receive a written request, we will provide the Individual with the accounting within sixty (60) days. If we cannot meet the 60-day deadline, we may extend the period for up to an additional thirty (30) days. In that event, we will give the Individual advance written notice of the extension and provide a statement of the reason(s) for the delay.
H. **Cost**  
An Individual will not be charged for the first accounting in any 12-month period. We may charge a reasonable, cost-based fee for each subsequent request for an accounting. In that case, we will provide the Individual, in advance, with an estimate of the fee and they will be given an opportunity to withdraw or modify their request in order to avoid or reduce the fee.

I. **Documentation**  
We will document and retain the following information:

- Relevant details regarding our disclosures of Protected Health Information;
- A copy of any accounting provided to an Individual; and
- The titles of the persons or offices responsible for receiving and processing requests for an accounting by Individuals.

J. **Complaints**  
Individuals who believe their HIPAA privacy rights have been violated have the right to file a complaint with the Secretary of the U.S. Department of Health and Human Services, 200 Independence Ave., S.W., Washington, D.C. 20201, or Company's Privacy Officer at 4055 Valley View Lane, Suite 400, Dallas, TX 75244, 1+(214) 279-8063 eFax. The complaint should be in writing, either in paper or in electronic format, and generally describe the acts or omissions believed to be in violation of the Individual's rights. Individuals will not be retaliated against for filing a complaint.

V. **MEMBERS OF THE WORKFORCE – TRAINING & CONDUCT**

A. **Privacy Obligation – Members of the Workforce**  
Our compliance with the HIPAA Privacy Standards requires the assistance, involvement, and education of all our members of the Workforce. Workforce (defined above) members are all those Individuals who act on our behalf, perform work for us, and act at our direction, facilitating our normal business operations. Persons who fall within this category include employees, volunteers, trainees, medical residents, independent contractors and leased or temporary workers.

B. **Reasonable Safeguards against Unnecessary Use or Disclosure**  
We will put into place and maintain reasonable safeguards to guard against and minimize unnecessary disclosures, or disclosures that occur incidentally in the workplace. These safeguards will involve our physical facilities, general operations, training, and policies and procedures.

C. **Reporting Violations**  
A member of the Workforce who witnesses or discovers a possible impermissible use or disclosures of Protected Health Information is **required** to immediately report the matter to Company’s Privacy Officer or other appropriate agent within that department. The report should be submitted in writing and provide the relevant identifying and descriptive
facts (i.e., names, date, time, location, other witnesses, substance of the violation, etc.). The reporting obligation extends to possible impermissible uses and disclosures by (i) other members of the Workforce and (ii) third parties, such as Business Associates.

D. **Training**

Company provides training to all members of the Workforce. The Human Resources, Compliance, Legal, Technology Departments, and other Company departments shall coordinate the delivery and documentation of all training required by the Privacy and Security Rule. Such training shall be specific to the Workforce members’ responsibilities as necessary and appropriate to carry out their functions, shall be prepared and revised to meet the specifications of this Policy regarding training, and shall include the contents of this Policy and all related implementing policies.

Areas of training include, without limitation:

- What constitutes Protected Health Information;
- Company HIPAA Privacy and Security Rule Policies;
- How to respond to an impermissible access, use, or disclosure;
- Permitted and required uses and disclosures;
- Minimum Necessary Standard;
- Disclosures requiring an authorization or consent;
- Interaction with Business Associates and other third parties;
- Document creation, retention and security;
- Handling requests, objections, complaints and related matters; and
- Communication and notices regarding policies, procedures and related matters.

All Workforce members receive training meeting the requirements of the Privacy and Security Rule during initial employee onboarding and no later than ten (10) days of employment. Said training is conducted by the Human Resources Department in coordination with other Company departments.

Retraining will take place at least annually and additionally where indicated through performance monitoring, auditing, and oversight functions. Further, the Privacy and/or Security Officer, in consultation with the Human Resources Department and other Company departments, shall ensure that further training is provided to any Workforce member whose functions are affected by any material change in policies or practices required by the Privacy and Security Rule. Company shall maintain documentation of all training required by the Privacy and Security Rules and this Policy.

E. **Sanctions**

Members of the Workforce who violate our Privacy Policy by making impermissible, non *de minimis* uses or disclosures of PHI are subject to sanctions in accordance with the Company’s progressive discipline policy, which may include termination of employment.
F. **Exception to Sanctions**
Sanctions cannot be applied to employees who use or disclose Protected Health Information because they reported, in good faith, unlawful or unethical workplace conduct or conduct that violates clinical or professional standards or endangers patients, workers or the public. This exception only applies if:

- The report was made to an appropriate health oversight agency, public health authority or health accreditation organization with jurisdiction or authority to investigate, supervise or enforce standards against us; or

- The report was made to an attorney of the reporting Workforce member or Business Associate for the purpose of allowing the Workforce member or Business Associate to consider legal options regarding the subject of the report.

VI. **CREATING AND MAINTAINING PRIVACY COMPLIANCE RECORDS**

A. **Creation of Privacy Records**
   1. **Internal Records.** We are required by law and our own policies to create certain records relating to implementation and maintenance of our privacy compliance program. Where possible, these records should be maintained in a central and secure location. The Privacy Officer is responsible for ensuring our compliance with the appropriate record keeping obligations.

   2. **Matters that Require and Individual’s Written Submission.** An Individual may be required to submit certain matters to us in writing, such as a complaint or request for amendment. When possible, the intake employee should provide the Individual with the appropriate form. The intake employee should also ensure that the form is fully and properly completed.

   3. **Matters that Only Require an Individual’s Verbal Statement.** An Individual is not always required to submit a request in written form. In those instances, the intake employee should encourage the Individual to make the submission in writing and use the appropriate form. If, however, the Individual refuses, the intake employee should fill in the appropriate form or otherwise document the relevant and necessary details.

B. **Retention and Maintenance Record – Overview**
We are required by law to maintain copies of the following types of documents in written or electronic format:

- Policies and Procedures;
- Communications; and
- Records of actions, activities or designations, as required by law.

C. **CMS Retention Period**
We are required by CMS to retain a record for ten (10) years from the date of its creation or the date when the record was last in effect, whichever is later. We may be required to maintain certain records longer under applicable state law or customer contract.

D. **Storage and Protection**
Where possible, all compliance records should be maintained in a central and segregated location. Reasonable security measures will be taken to ensure that only authorized and necessary employees will have access to the records.

**Note:** See LE-01 Company Records Management Policy for complete details.

VII. **REQUESTS FOR ACCESS TO RECORDS**

A. **No Right of Access to Certain Records**
An Individual does not have a right of access under federal law to certain record sets. If an Individual submits a request that includes both prohibited and lawfully accessible information, we will exclude the prohibited information and give the Individual access to the remaining requested information.

Access is not permitted to the following record sets or under the following circumstances:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access request is reasonably likely to endanger the life or physical safety of the Individual or another person;
- The requested Protected Health Information makes reference to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the other person;
- The request for access is made by an Individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the Individual or another person;
- The record set contains psychotherapy notes;
- The record set includes information that is compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
- When access is prohibited by the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a;
- Protected health information that is exempt from the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, pursuant to 42 CFR 493.3(a)(2);
- Where the requested information is subject to the Privacy Act, 5 U.S.C. §552a, and denial of access is proper under the Privacy Act; or
- The requested Protected Health Information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
1. **Time-Frame.** Once the Individual submits a written request, we will act on it within thirty (30) days unless the information they seek is not maintained or kept on-site. In that instance, we will act on the request within sixty (60) days. If we are unable to act within the 30-day (or 60-day, if applicable) time frame, we may extend the period once for no more than thirty (30) days provided that, within the original time period, we notify the Individual in writing of the new response deadline and the reasons for the delay.

2. **Review Process.** Our Privacy Officer or other designated agent will review the request and the applicable records to determine whether they are subject to access, in whole or in part. If necessary, the reviewing agent will seek the guidance of a licensed health care professional when making this determination.

3. **Request Granted.** If we grant the request, in whole or in part, we will notify the Individual of our decision, in writing, and provide the requested copy and/or, if possible, the form of access requested.

4. **Cost.** If the Individual requests a copy, we may charge them a reasonable, cost-based fee. In that case, we will provide the Individual, in advance, with an estimate of cost.

5. **Information Not Maintained by Us.** If we do not maintain the information the Individual seeks, but know where it is maintained, we will inform the Individual where to direct his or her request for access.

6. **Request Denied.** If we deny the request, in whole or in part, we will notify the Individual in writing and include a plain language description of the basis for the decision, the Individual’s rights, if any, to a review of our decision, and a description of the complaint procedures established under federal law.

**B. Individual’s Rights Following Denial**

1. **Denials Subject to Review.** An Individual only has a right to request a review of our decision to deny access if the denial is based on one of the following reasons:
   a) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Individual or another person;
   b) The requested Protected Health Information makes reference to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the other person; or
   c) The request for access is made by an Individual’s personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the Individual or another person.
2. **Time for Requesting Review.** Any request for review of our denial must be submitted within twenty-one (21) days of the Individual’s receipt of notice of our decision to deny the request. An Individual who submits a request after the expiration of twenty-one (21) days will be deemed to have waived his or her rights to review and the request will be automatically denied.

3. **Form of Request.** The request may be made either orally or in writing, although the Individual should be encouraged to complete our form. If the request is made orally, the intake employee should document date of the request, the identity of the requesting Individual, the intake employee’s own name, and any other relevant information.

4. **Reviewing the Decision.** Following the request we will designate a licensed health care professional, who did not participate in the original decision to deny access, to act as the reviewing official and refer the matter to him/her for review and determination. We will provide or deny access in accordance with the determination.

C. **Complaints**

   Individuals who believe their HIPAA privacy rights have been violated have the right to file a complaint with the Secretary of the U.S. Department of Health and Human Services, 200 Independence Ave., S.W., Washington, D.C. 20201, or Company’s Privacy Officer at 4055 Valley View Lane, Suite 400, Dallas, TX 75244, 1+(214) 279-8063 eFax. The complaint should be in writing, either in paper or in electronic format, and generally describe the acts or omissions believed to be in violation of the Individual’s rights.

D. **No Retaliation**

   We will not retaliate against an Individual for filing a complaint or requesting a review of our decision.

VIII. **RESOLUTION OF OBJECTIONS AND COMPLAINTS**

A. **Individuals’ Right to Object and Complain**

   Individuals have the right to file objections or complaints regarding our handling of their Protected Health Information. Our obligation to take action(s) in response to an objection or complaint depends on the nature of the objection or complaint.

B. **Form of Complaint or Objection**

   Whenever possible, Individuals should be urged to file complaints or objections in written or electronic format (a written complaint or objection may be required in certain instances). If the complaint or objection is made verbally, the intake employee should, as soon as possible, document the relevant facts, including the substance of the complaint or objection, the date it was submitted, the identity of the Individual, the identity
of the intake employee, and any other fact that might be relevant to a resolution of the complaint or objection.

C. **Specific Instances**
   1. **Impermissible Use or Disclosure by a Business Associate**
      - **Form** – A complaint involving Business Associate’s alleged impermissible use or disclosure of Protected Health Information may be made verbally or in writing, although the Individual should be encouraged to provide a written complaint or objection.
      - **Investigation** – Following receipt of the complaint, our Privacy Officer or other qualified and duly designated agent will conduct a thorough investigation of the complaint to determine its validity. The investigation should be commenced within 7 business days of the receipt of the complaint and be completed within 45 days, unless completion within such a time frame is unreasonable. The investigator should document all steps of the investigative process.
      - **Violation Found** – If the investigation establishes that the Business Associate improperly used or disclosed Protected Health Information or otherwise violated the terms of its Agreement, we will take reasonable steps, depending on the situation, to end the violation and prevent similar future occurrences.
      - **Re-occurring Violation** – If the violation or similar improper use or disclosure occurs despite our having taken reasonable steps to cure the problem, we will terminate the contract or arrangement with the Business Associate. If termination of the contract or agreement is not feasible, we will report the problem to the Department of Health and Human Services Office for Civil Rights.
      - **Contractual Provisions Control** – Prior to addressing a contractual violation or impermissible use or disclosure, the applicable Business Associate should be carefully reviewed to determine the proper procedure and our obligations with regard to providing notice to the Business Associate.
      - **Notifying the Individual** – When practical, we will provide a written response to the complaint within a reasonable time period. The response should acknowledge our receipt of the complaint and generally describe an action taken in response to the complaint.

D. **Request for Amendment**
   The procedures for responding to an Individual’s objection or complaint relating to our handling of the Individual’s request for amendment of Protected Health Information are presented in detail in our policy on Amendment Requests set forth above.

E. **Request for Access**
   The procedures for responding to an Individual’s objection or complaint relating to our handling of the Individual’s request for access to Protected Health Information are presented in detail in our policy on Requests for Access set forth above.

F. **Request for Accounting of Disclosures**
The procedures for responding to an Individual’s objection or complaint relating to our handling of the Individual’s request for an accounting of our disclosures of Protected Health Information are presented in detail in our policy on Accounting of Disclosures set forth above.

G. **General Complaints**
Complaints regarding impermissible use or disclosure by a Member of the Workforce fall into this category. Individuals who believe their HIPAA privacy rights have been violated have the right to file a complaint with the Secretary of the U.S. Department of Health and Human Services, 200 Independence Ave., S.W., Washington, D.C. 20201, or Company’s Privacy Officer at 4055 Valley View Lane, Suite 400, Dallas, TX 75244, 1+(214) 279-8063 eFax. The complaint should be in writing, either in paper or in electronic format, and generally describe the acts or omissions believed to be in violation of the Individual’s rights.

When practical, we will provide a written response to any complaint within a reasonable time period. The response should acknowledge our receipt of the complaint and generally describe any action taken in response to the complaint.

H. **No Retaliation**
Individuals will not be retaliated against for filing a complaint or objection.

IX. **BREACHES**

A. **General Policy**
Company will notify Individuals and or Covered Entities in compliance with federal law and the terms of any Business Associate Agreement or other Services Agreement if unsecure PHI is breached.

B. **What Information is subject to this Policy?**
This policy only applies to “unsecure” PHI, which includes information that is not either encrypted under specific standards adopted by NIST or destroyed so that it cannot be read or reconstructed.

C. **What is a Breach, generally?**
A Breach will occur if the following three requirements are met:
1. Information is “unsecure” as described above;
2. Information was used or disclosed in an “unauthorized” manner—this means that the information was used or disclosed in a manner that is not permitted under HIPAA, including a violation of the Minimum Necessary rule; and
3. The use or disclosure poses a significant risk of financial, reputational, or other harm to the Individual.
Company will perform a risk assessment to determine if harm has occurred and review factors such as to whom the information was disclosed, the type of information disclosed, and what steps were taken upon discovery of the use or disclosure.

E. **Exceptions**
A use or disclosure does not occur if one of the following exceptions applies.

1. **Unintentional access by a Covered Entity’s or Business Associate’s employee.**
   This means access which is in good faith, within the employee’s course and scope of employment, and that does not result in further use or disclosure.

2. **Inadvertent disclosure from one Covered Entity or Business Associate employee to another similarly situated employee.** The information must not be further used. “Similarly situated” means both employees must be authorized to access the information. For example, a doctor and a billing employee may be similarly situated in that they are both authorized to view PHI, but a doctor and a receptionist might not be.

3. **The recipient would not reasonably have been able to retain the information.**
   For example, where health information is mailed to the wrong Individual. If the envelope is returned unopened, the plan could determine that the recipient did not retain the information.

F. **When is Notice Required?**
If there is a confirmed Breach, Company must notify the client health plan and/or the Individual, dependent upon the facts of the relationship and contractual obligations in place, without unreasonable delay, but no later than sixty (60) days after the discovery of the breach. However, Business Associate Agreements generally require notice to the health plan within a few days of discovery of a potential Breach. A Breach is considered discovered on the first day it is known to any member of the Workforce (other than the person who committed the Breach), or the date it would have been known if we had exercised reasonable diligence.

G. **Form of the Notice**
The notice must be written in “plain language” and contain:

- A brief description of what happened, including the date of the Breach and date of discovery;
- The types of PHI involved (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps the Individual should take to prevent themselves from potential harm;
- A brief description of steps Company is taking to investigate, mitigate losses, and protect against further Breaches; and
- Contact information for questions, including a toll-free telephone number, email address, website, or postal address.
Notice must be sent to the Individual’s last known address or by email if the Individual agrees. Notices to minors generally can be sent to parents and notices to deceased Individuals generally can be sent to next of kin or a personal representative, consistent with the HIPAA privacy rules.

E. **Insufficient Contact Information or Notification is Returned as Undeliverable**

If insufficient or out-of-date contact information precludes Individual notice, Company will provide a substitute form of notice.

1. **If fewer than ten (10) Individuals are involved.** The substitute notice may be an alternative form of notice that is reasonably calculated to reach the Individuals, such as by telephone, email, or posting on the Covered Entity’s website.

2. **If ten (10) or more Individuals are involved.** Company will either post the notice on its homepage for ninety (90) days or provide notice in major print or broadcast media in the geographic areas where affected Individuals are likely to reside. Under either approach, Company will maintain a toll-free number for ninety (90) days so Individuals can ask questions. For website posting, the notice will be prominent so that it is noticeable given its size, color, and graphic treatment in relation to other parts of the page, and worded to convey the nature and importance of the information. The notice will be included on both the homepage and “landing page” for existing account holders.

F. **Notice to HHS**

1. **Where a Breach involves 500 or more people.** Company will notify the Secretary of HHS immediately. “Immediately” means contemporaneously with the Individual notice (that is, within sixty [60] days of confirmation of said Breach).

2. **Where a Breach involves less than 500 people.** Company will maintain a log of security Breaches and submit it to HHS on an annual basis. The log will be filed within sixty (60) days after the end of the calendar year.

X. **REPORTING/QUESTIONS/ENFORCEMENT**

A. **Reporting**

Suspected or known violations of this policy, whether accidental or intentional, must be reported immediately to your supervisor and the Privacy Officer, Security Officer, or Hotline defined above.

B. **Questions**

Questions concerning the applicability of or exception to this policy can be directed to the Privacy Officer.

C. **Non-Compliance**
Anyone found to have violated this policy will be subject to disciplinary action, up to and including termination.

Accountable for Policy Implementation and Maintenance: Privacy Officer & Security Officer