ARK LABORATORY, LLC D/B/A HELIX DIAGNOSTICS ("COMPANY")
HIPAA PRIVACY POLICES AND PROCEDURES

DEFINITIONS

Unless otherwise provided, the definitions set forth below apply to all of the HIPAA Privacy Policies and Procedures reflected herein. Any capitalized terms used and not defined herein shall have the meanings ascribed to them pursuant to HIPAA.

Business Associate means a person or entity who is not a member of Company's workforce and performs or assists in the performance of a function or activity for or on behalf of Company regarding healthcare operations or payment purposes or for any other function or activity involving PHI.

Company means Ark Laboratory, LLC d/b/a Helix Diagnostics.

Designated Record Set means a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about individuals maintained by or for a covered Health Care Provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about Individuals. The term "records" in this definition means any item, collection, or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for a covered entity.

Disclosure (or Disclose) means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Health Care Operations means:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
- Reviewing the competence or qualifications of health care providers, including evaluation of providers' performance;
- Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business management and general administrative activities, including those related to implementing and complying with the HIPAA Privacy Rule customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity; and
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity.

HIPAA means the Privacy Standards of the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations, 45 CFR Parts 160 and 164, as they are amended from time to time.

Individual means the person who is the subject of PHI.

Payment means:

- Obtaining premiums or to determine or fulfill its responsibility for coverage;
- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims provision of benefits under a health plan;
- Obtaining reimbursement for health care;
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
- Disclosures of certain elements of PHI to consumer reporting agencies

Privacy Official means the person designated by Company with overall responsibility for Company's compliance with the HIPAA Privacy and Breach Notification Rules. The Privacy Official is responsible for the development and implementation of the Policies and Procedure reflected herein. The Privacy Official may delegate responsibilities or tasks described in these Policies and Procedures as needed and as appropriate, provided he or she maintains oversight of such delegated responsibilities or tasks.

Protected Health Information ("PHI") has the same meaning as in 45 CFR 164.103.

Required by Law means a mandate contained in law that compels Company to make a use or disclosure of PHI and that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary means the Secretary of the Department of Health and Human Services.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary. Essentially, secured PHI is encrypted or has been destroyed beyond the ability to recover (e.g. shredded).

Use (or Uses) means, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

NOTICE OF PRIVACY PRACTICES - POLICY (1) AND PROCEDURE (1.1)

1. **Policy:** It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.520.

1.1 **Procedure**:

a. Company will:
   i. Maintain a Notice of Privacy Practices ("NPP");
   ii. Write the NPP in plain language;
   iii. Provide the NPP to any Individual that requests a copy thereof;
   iv. Obtain an Individual's written acknowledgement of their receipt of the NPP, or document that a reasonable attempt was made by Company to obtain the Individual's acknowledgement;
      1. Any such written acknowledgment of receipt or documentation of a reasonable attempt to obtain the Individual's written acknowledgment will be maintained in accordance with Company's "HIPAA Retention Policy and Procedure."
   v. Not less than once annually, review and, if needed, revise the content of the NPP, including identifying those revisions that constitute a Material Change to Company's privacy practices, if any;
      1. In instances where a Material Change has occurred, the NPP will be re-distributed (i.e., made available upon request) to Individuals as soon as reasonably possible.
      2. Material Changes to the NPP will not be implemented prior to the effective date of the revised NPP.
      3. Any revision which is not considered a Material Change may be implemented prior to the effective date of the revised NPP, unless otherwise prohibited by law.
   vi. Track and document each version of the NPP, including the effective date of the same.
      1. Any changes to the NPP, non-material or material, will be tracked and documented.
      2. All versions of the NPP will be maintained in accordance with Company's "HIPAA Retention Policy and Procedure."
   vii. Refer inquiries regarding the NPP to the Privacy Official.
   viii. To the extent that Company maintains a website that provides information regarding its services to Individuals, Company will prominently post its NPP on the website and will make the NPP electronically available to Individuals thereon.
   ix. To the extent that Company's applicable responsibilities under 45 CFR 164.520 and 45 CFR 164.530 are carried out by a Business Associate, confirm, no less than once annually, that the Business Associate is in compliance with the same.

Definitions applicable to Policy (1) and Procedure (1.1):

Material Change means a modification that would create a new category of use or disclosure of PHI that may be made without Individual authorization or a material enhancement, change, or reduction of Individual rights.

Notice of Privacy Practices means a document that describes how Company will use and disclose Individual PHI, informs Individuals of their rights regarding PHI and Company's legal duties regarding the same.

Effective Date: JUNE 24, 2021

PERSONAL REPRESENTATIVES - POLICY (2) AND PROCEDURE (2.1)

2. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH and state law requirements regarding 45 CFR 164.502(g).

2.1 **Procedure**:

a. **In General, and Adults**

i. Company, or its Privacy Official, will verify both the identity and authority of an individual requesting an adult Individual's PHI before disclosing the Individual's PHI to the individual.

1. If the individual is unknown to Company, Company will verify the identity of the individual by one or more of the following methods:
    a. Reviewing a valid photo identification of the individual; and/or
    b. Requiring the individual to correctly answer questions about the Individual, including data contained in the Individual's records that may identify the individual as an appropriate representative, if any (e.g., identification of family members, emergency contacts, etc.).
2. Company will require the individual to provide Company with appropriate documentation that confirms he or she is authorized to receive the Individual's PHI by:
    a. Requesting the individual to provide Company with a HIPAA-compliant authorization that has been signed by the Individual, and confirming the accuracy of the Individual's signature thereon; or
    b. Requesting the individual provide Company with documentation that confirms that they have legal authority, pursuant to applicable state law, to act on the Individual's behalf and receive the Individual's PHI (e.g., durable power of attorney, court-appointed legal guardianship, etc.).

ii. In instances where Company has verified the identity and authority of an individual acting on behalf of an Individual, Company will treat the individual as the Individual's personal representative.

iii. Except for certain situations described in this Procedure, Company will treat an Individual's personal representative as if they are the Individual on whose behalf the personal representative is permitted to act for HIPAA purposes (e.g., requesting access, requesting restrictions, requesting amendments, signing authorizations, etc., on the Individual's behalf).

iv. Company will only disclose the PHI to an Individual's personal representative that is relevant to their personal representation.

v. Company, its workforce members, and others acting on Company's behalf will consult with Company's Privacy Official and/or legal counsel if there are any questions regarding whether or not an individual is a personal representative of an Individual.

b. **Emancipated Minors**
   i. Company will request documentation from an emancipated minor (who is an Individual) that evidences their emancipation (e.g., a court order of emancipation) before treating the minor as an adult for HIPAA purposes.

c. **Unemancipated Minors**
   i. Company will treat a minor's parent(s), guardian or other person responsible for the minor (as authorized by applicable law) as the minor's personal representative unless:
      1. The minor is emancipated;
      2. The minor, pursuant to applicable state or other law, is permitted to consent to the subject health care service, no other consent is required by law and the minor has not requested that their parent be treated as a personal representative; or
      3. The minor's parent, guardian or other person responsible for the minor (as authorized by applicable law) entered into an agreement of confidentiality with respect to the subject health care service.
         a. If Company is informed by an Individual's health care provider of an agreement of confidentiality as described above, Company's Privacy Official will, upon consultation with the subject health care provider, determine whether or not it is appropriate for Company to adhere to said agreement.
   ii. Notwithstanding paragraph 2.1.c.i. above, Company may disclose PHI to a minor's parent, guardian or other person responsible for the minor (as authorized by applicable law) as necessary in order to avert a serious and imminent threat to the health or safety of the minor or as required by state law.

d. **Deceased Individuals**
   i. To the extent a deceased Individual's executor, administrator, or other person that has the authority under state law to act on the deceased Individual's behalf or on behalf of the Individual's estate, Company will treat the individual as the Individual's personal representative.

e. **Abuse, Neglect, or Endangerment**
   i. Notwithstanding applicable state law and this Procedure, Company may elect not to treat an individual as an Individual's representative if it has a reasonable belief that:
      1. The individual has or may subject the Individual to domestic violence, abuse or neglect; or
      2. Treating the individual as the Individual's personal representative could endanger the Individual; and

3. Company, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

Effective Date: **JUNE 24, 2021**

USE AND DISCLOSURE OF PHI NOT REQUIRING PATIENT AUTHORIZATION - POLICY (3) AND PROCEDURE (3.1)

3. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.506 and 45 CFR 164.512.

3.1 **Procedure**:

a. **Disclosures for Company's Treatment, Payment, and Health Care Operations Purposes**

i. Unless Company has agreed to a restriction, Company may, without the Individual's authorization or offering the Individual an opportunity to agree or object, use or disclose an Individual's PHI:

1. To carry out its own Treatment, Payment, or Health Care Operations activities (e.g., disclosure of Individual information to billing companies or collection agencies for Payment purposes);
2. To a health care provider, for the health care provider's own Treatment or Payment purposes; and/or
3. To another covered entity for the covered entity's own Treatment or Payment purposes (e.g., disclosure of member information to other health plans for coverage determinations, eligibility determinations, medical necessity/appropriateness review, justification of charges, utilization review, pre-certification, or preauthorization), and for certain Health Care Operations purposes if both Company and the covered entity have or had a relationship with the Individual and the disclosure pertains to the relationship.

b. **Other Uses and Disclosures Not Requiring Individual Authorization**

i. Company may, without the Individual's authorization or offering the Individual an opportunity to agree or object, use or disclose an Individual's PHI:

1. When Required by Law;
2. For public health activities to Public Health Authorities (e.g., the Food and Drug Administration, the Centers for Disease Control, etc.), provided:
    a. The use or disclosure is to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, disability, or to receive reports of child abuse or neglect.
    b. To notify a person that he or she has been exposed to a communicable disease (if otherwise permitted by law to make this disclosure).
    c. To report an adverse event to the Food and Drug Administration (FDA) with respect to an FDA-regulated product; to track FDA-regulated products; to enable

product recalls, repairs, or replacements, or lookback; or to conduct post marketing surveillance.

d. The use or disclosure is limited to proof of immunization related to a student or prospective student, provided that such use or disclosure is approved in advance by Company's Privacy Official and legal counsel;

3. To appropriate government authorities in order to report abuse, neglect, or domestic violence, provided that such use or disclosure is approved in advance by Company's Privacy Official and legal counsel;
4. To a health oversight agency for the agency's oversight activities that are authorized by law, including: audits, civil, administrative or criminal investigations, proceedings, or actions, inspections, licensure or disciplinary actions, or other oversight activities;
5. For judicial and administrative proceedings in response to an:
    a. order of a court, administrative tribunal, provided the information disclosed is consistent with the order;
    b. subpoena, discovery request or other lawful process (not accompanied by a court order) provided:
        i. Company has received certain satisfactory assurances from the party seeking the Individual's PHI (i.e., that the Individual has been notified about the court proceeding or that the parties have entered into a protective order with regard to the Individual's PHI).
    c. In the event that Company receives a request for Individual PHI pursuant to this paragraph 3.1.b.i.5 of this Procedure, Company will consult with its Privacy Official and legal counsel prior to disclosing the PHI;
6. For certain law enforcement purposes (e.g., certain wound reporting, responding to subpoenas, responding to requests regarding suspected victims of crimes, reporting crimes on the premises or in emergency situations), including limited identifying and location information requested by a law enforcement official, provided that such use or disclosure is

approved in advance by Company's Privacy Official and legal counsel;

7. To organ procurement agencies for organ donation and transplantation purposes;
8. To coroners and medical examiners in order to identify a deceased Individual, determining the Individual's cause of death, or other duties required by law;
9. To funeral directors, as necessary, so they may carry out their duties;
10. For certain Research uses;
11. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
12. For specialized government functions, including information related to armed forces personnel for activities deemed appropriate by military command authorities;
13. For national security purposes to authorized federal officials;
14. To correctional institutions or law enforcement officials having lawful custody of an inmate, in instances where such a disclosure is appropriate and necessary;
15. To the extent necessary to comply workers' compensation laws
16. To Business Associates, in accordance with Policy 10 and Procedure 10.1;
17. To Individuals upon their request pursuant to Policy 8 and Procedure 8.1; and/or
18. When incidental to a use or disclosure that is otherwise permitted or required.

ii. Prior to disclosing PHI for one or more of the purposes reflected in paragraph 3.1.b.i of this Procedure, Company's Privacy Official or legal counsel will be consulted and will ensure that the disclosure meets all requirements related to HIPAA and other applicable law.

iii. Disclosures of PHI made pursuant to this Procedure will conform to the requirements of Policy 6 and Procedure 6.1.

iv. Disclosures of PHI made for one or more of the purposes reflected in paragraph 3.1.b.i of this Procedure will be tracked and documented in accordance with the requirements of Policy 8 and Procedure 8.1(j) (Accounting of Disclosures).

Definitions applicable to Policy (3) and Procedure (3.1):

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Effective Date: **JUNE 24, 2021**

USE AND DISCLOSURE OF PHI REQUIRING AN OPPORTUNITY FOR THE PATIENT TO AGREE OR OBJECT – POLICY (4) AND PROCEDURE (4.1)

4. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.510.

4.1 **Procedure**:

a. Company will provide all Individuals with an opportunity to agree or object to uses and disclosures of PHI described in this Procedure unless otherwise specified.
b. Company will document Individual responses regarding whether the Individual has agreed or objected to the uses and disclosures of PHI described in this Procedure.
c. Company will honor an Individual's objections subject to the exceptions listed in this Procedure and will not disclose the Individual's PHI unless Required by Law or otherwise permitted.
d. Company's Privacy Official will ensure Company's compliance with this Procedure.
e. **Uses and Disclosures to Family, Friends, and/or Persons Involved in the Individual's Care**
    i. In accordance with this Procedure, Company may disclose, to an Individual's family member, friend, or any other person identified by the Individual, PHI that is directly relevant to the person's involvement in the Individual's health care or payment related to the Individual's health care, including information regarding the Individual's death, unless doing so is inconsistent with the Individual's prior expressed preferences.
    ii. If an Individual is present for, or otherwise available prior to, a use or disclosure permitted by this Policy and has the capacity to make health care decisions, Company may use or disclose the PHI if it:
        1. Obtains the Individual's agreement;
        2. Provides the Individual with the opportunity to object to the disclosure, and the Individual does not express an objection; or
        3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the Individual does not object to the disclosure.
    iii. If an Individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the Individual's incapacity or an emergency circumstance, Company may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the Individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the Individual's care or payment related to the Individual's health care or needed for notification purposes. Company may use professional judgment and its experience with common practice to make reasonable

inferences of the Individual's best interest in allowing a person to act on behalf of the Individual to pick up filled prescriptions, medical supplies, or other similar forms of PHI.

iv. If an Individual is deceased, Company may disclose to a family member, or other persons who were involved in the Individual's care or payment for health care prior to the Individual's death, PHI of the Individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the Individual that is known to Company.

f. **Uses and Disclosures Disaster Relief Purposes**

i. Company may use or disclose an Individual's PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures of PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the Individual, or another person responsible for the care of the Individual of the Individual's location, general condition, or death.

ii. The requirements set forth in paragraphs 4.1(e)(ii), (iii), and (iv) shall apply to the extent that Company, in the exercise of its professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

Effective Date: **JUNE 24, 2021**

USE AND DISCLOSURE OF PHI REQUIRING PATIENT AUTHORIZATION - POLICY (5) AND PROCEDURE (5.1)

5. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.508.

5.1 **Procedure**:

a. Unless otherwise permitted by HIPAA or these Policies and Procedures, Company will obtain an Individual's signed HIPAA-compliant authorization before disclosing PHI, including for certain purposes involving:
   i. Marketing;
   ii. Fundraising;
   iii. Research; and
   iv. Disclosure of Psychotherapy notes.

b. Company will ensure that disclosures of PHI made pursuant to Individual authorization are limited to the amount and type of PHI reflected on the authorization.

c. **Marketing**
   i. Company may access and/or use or disclose PHI for Marketing (see definition of Marketing below) purposes to Individuals for Treatment, certain Health Care Operations purposes or to describe a health-related Treatment or service provided or offered under the Company, **unless** the Company receives direct or indirect remuneration for making the communication - in which case written authorization is required.
   ii. Company will obtain written authorization from Individuals if Company receives any direct or indirect remuneration (e.g., payment) from, or on behalf of, a third party in exchange for sending the communication and the communication is intended to encourage purchase or use of a product or service offered by the third party.
   iii. In the event that an authorization is required for Marketing purposes and involves remuneration, the authorization will state that remuneration is involved.

d. **Research**
   i. Company will obtain written authorization prior to using or disclosing Individual PHI for Research purposes, unless:
      1. The Company has received a written waiver of authorization from an Institutional Review Board or Privacy Board overseeing the Research;
      2. The Individual(s) is deceased, and the use and disclosure of the PHI is necessary for and will be solely use for Research purposes; or
      3. The Individual PHI will only be used for activities that are preparatory to Research (e.g., to identify potential research subjects).

e. **Sale of PHI**

i. Company will obtain written authorization from Individuals prior to selling Individual PHI. The authorization will state that Company will receive remuneration in connection with the sale, if any.

f. **Psychotherapy Notes**

i. Company will obtain written authorization prior to disclosing Individual Psychotherapy Notes unless:

1. Company is carrying out the following Treatment, Payment, or Health Care Operations:
    a. Use by the originator of the Psychotherapy Notes for Treatment;
    b. Use or disclosure by Company for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
    c. Use or disclosure by Company to defend itself in a legal action or other proceeding brought by the individual; or
2. A use or disclosure that is: (i) required by the Secretary or applicable law, or (ii) permitted with respect to a health oversight agency as it pertains to the oversight of the originator of the psychotherapy notes, disclosures to coroners or medical examiners, or if Company in good faith believes 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 and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

ii. Company will consult with its Privacy Official or legal counsel for all other disclosures concerning Individual Psychotherapy Notes.

g. **Authorization Requirements**

i. Authorizations provided to Individuals by Company must be written in plain language and reflect the following:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may disclose the PHI to;
4. A description of each purpose of the requested use or disclosure. The statement “at the request of the Individual” is a sufficient description of the purpose when an Individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;

5. An expiration date or an expiration event that relates to the Individual or the purpose of the use or disclosure. Authorizations may permit the Disclosure of subsequent / future medical records, although Company may limit the time frame (i.e., Disclosure of all medical records related to an Individual's workers' compensation claim);
6. A statement regarding the Individual's right to revoke the authorization in writing and the exceptions to the right to revoke;
7. A description on how the Individual may revoke the authorization;
8. A statement that Company will not condition treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization, except as permitted by law;
9. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by HIPAA; and
10. The signature of the Individual and date. In the event that the authorization is signed by a personal representative of the Individual, the authorization must contain a description of the representative's authority to act on behalf of the Individual. HIPAA allows for the signature of a personal representative if the Company would recognize the personal representative as a person the Individual would like to authorize to receive PHI (e.g., health care power of attorney, court appointed legal guardian, a parent, etc.).

h. **Conditioning Authorizations**
   i. Company will not require an Individual to sign an authorization as a condition for Treatment, Payment, enrollment in the health plan, or eligibility for benefits, except:
      1. Company may condition the provision of Research-related treatment on provision of an authorization for the use or disclosure of PHI for such research; and
      2. Company may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.
   ii. Company will consult with its Privacy Official and/or legal counsel before requiring an Individual to sign an authorization for use or disclosure of the Individual's PHI for any other purpose.

i. **Combining Authorizations**
   i. Company will not combine authorizations with other documents to create a compound authorization without first consulting with its Privacy Official and legal counsel.

j. **Revocation of Authorization & Defects**
   i. Individuals may revoke their authorization at any time provided that the revocation is in writing.

ii. Company will not be accountable for disclosures made prior to the Individual's revocation.
iii. Company will not rely on any Individual authorization that Company knows to be defective, i.e., that is expired, revoked, filled out incorrectly or incompletely, contains information that Company knows to be false, or that does not contain the elements reflected in paragraph 5.1.g of this Procedure.

k. **Copy to the Individual**
   i. If Company seeks an authorization from an Individual for the use or disclosure of the Individual's PHI, Company will provide a copy of the authorization to the Individual, which includes the Individual's signature.

Definitions applicable to Policy (5) and Procedure (5.1):

Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an Individual.

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Unless financial remuneration is received, marketing does **not** mean communications made by Company that:

- Are Face-to-face to an Individual;
- Are promotional gifts of nominal value;
- Are made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the Individual, only if any financial remuneration received by the Company in exchange for making the communication is reasonably related to the Company's cost of making the communication;
- Are made for the following treatment and health care operations purposes, except where the Company receives financial remuneration in exchange for making the communication:
  - For treatment of an Individual by a health care provider, including case management or care coordination for the Individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the Individual;
  - To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

- For case management or care coordination, contacting of an Individual with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

Psychotherapy Notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy Notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Effective Date: **JUNE 24, 2021**

MINIMUM NECESSARY - POLICY (6) & PROCEDURE (6.1)

6. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.502(b).

6.1 **Policy**:

a. Company will make reasonable efforts to limit the use, disclosure, access to or requests for PHI to the minimum necessary.
b. Company will verify the identity of a requestor of PHI if the requestor is unknown to Company.
c. **Internal Use**
    i. Company's Privacy Official will make reasonable efforts to ensure workforce members' and others' access and use is limited to PHI that is required to carry out their duties.
    ii. The following categories of work force members will have the following levels of access to PHI necessary to carry out their duties:

Role (category of individual within facility)	Patient Name, Demographics, Scheduling information	Billing/financial and insurance information	Procedure/ Diagnosis information	Medical Notes (e.g. physician/ provider notes)
Owner	Full	Full	Full	Full
VP	Full	Full	Full	Full
Director	Full	Full	Full	Full
Manager	Full	Full	Full	Partial
Supervisor	Full	Partial	Partial	Partial
Lead	Full	Partial	Partial	Partial
Technologist	Partial	Partial	Partial	Partial
Lab Assistant	Partial	Partial	Partial	None

d. **Requesting PHI from Business Associates and other Covered Entities**
    i. Company will limit the PHI it requests from other covered entities to the minimum amount needed (e.g., requests will be as specific as possible).
e. **Disclosures to Third Parties**
    i. When responding to a request for PHI from a third party, Company will ensure that it only discloses the minimum amount of PHI necessary to fulfill the request.
    ii. Company's Privacy Official will determine if requests are considered "routine."
    iii. For requests that are considered "routine," Company is permitted to disclose the minimum amount of PHI necessary to fulfill the request, as

conveyed by the requestor (i.e., Company may disclose the amount of PHI requested).

iv. The Privacy Official will annually review the list of "routine" request recipients below to ensure that they should continue to be classified as "routine" recipients of PHI:
    1. Disclosures made to the Individual who is the subject of the PHI;
    2. Disclosures made in accordance with a valid authorization that complies with 45 CFR 164.508;
    3. Disclosures made to a health care provider for treatment;
    4. Disclosures made to a health plan or health care clearing house;
        a. This includes third-party payors to the extent needed or required by contracts or other agreements with said payor for either Company's or the payor's payment activities.
    5. The information is requested by a professional who is a member of Company's workforce or is a Business Associate of Company for the purpose of providing professional services to Company, if the professional represents that the information requested is the minimum necessary for the stated purpose(s);
    6. Disclosures that are Required by Law;
    7. Disclosures made to a public official or agency in accordance with applicable law, if the public official represents that the information requested is the minimum necessary;
    8. Disclosures made to the Secretary of the Department of Health and Human Services for the purposes of compliance and enforcement of HIPAA;
    9. Disclosures required for compliance with the privacy and security standards; and
    10. Other disclosures may be classified by the Privacy or Security Official as routine.

v. Non-routine requests for disclosure of PHI from third parties will be forwarded to and reviewed by the Privacy or Security Official prior to disclosing the PHI to the third party.
    1. The Privacy or Security Official will determine if such requests should be honored and the amount of PHI to be disclosed in connection with the request, consistent with the requirements this Procedure and HIPAA.

f. **Limited Data Sets**

i. To the extent that Company wishes to use or disclose PHI in the form of a Limited Data Set ("LDS") for Research, public health, or Health Care Operations purposes, Company will enter into a Data Use Agreement with the recipient prior to disclosing the LDS.
    1. To the extent possible, an LDS will be disclosed to recipients who request PHI for the purposes of Research, public health, or Health Care Operations.

ii. The LDS will exclude all of the direct and indirect identifiers of the Individual, and his or her relatives, employers, or household members indicated in the paragraph 6.1.g.i. of this Procedure below; however, the postal information regarding the town or city, state and zip code is permitted (excluding the postal street address).

iii. The Data Use Agreement must prohibit the recipient of the LDS from any use or disclosure of PHI for a purpose beyond the one(s) set forth in the Data Use Agreement.

g. **De-identified Information**

i. PHI will be considered de-identified if all of the following identifiers of the Individual (including the Individual's relatives, employers, or household members) have been removed:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (i) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people;
3. (ii) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
4. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
5. Telephone numbers;
6. Fax numbers;
7. Electronic mail addresses;
8. Social security numbers;
9. Medical record numbers;
10. Health plan beneficiary numbers;
11. Account numbers;
12. Certificate/license numbers;
13. Vehicle identifiers and serial numbers, including license plate numbers;
14. Device identifiers and serial numbers;
15. Web Universal Resource Locators (URLs);
16. Internet Protocol (IP) address numbers;
17. Biometrics identifiers, including finger and voice prints;
18. Full face photographic images and any comparable images; and
19. Any other unique identifying number, characteristic, or code.

Definitions applicable to Policy (6) and Procedure (6.1):

Data Use Agreement means a required agreement between Company and a Limited Data Set recipient setting forth the obligations regarding the use or disclosure of PHI contained in the Limited Data Set.

De-identify or **De-identification** means a data set whereby all 18 specific PHI identifiers have been removed from the data (i.e., refer to the detailed list below). As an alternative, less than all of the 18 specific identifiers are removed and an expert opines that the data cannot be Re-Identified. In either case, there is no reasonable basis to believe that the information in the data set can be used to identify an individual.

Limited Data Set or **("LDS")** means a data set for Use and Disclosure of PHI for the purposes of research, public health or health care operations that is not completely De-Identified. The data set excludes 16 specified identifiers in accordance with applicable law but includes complete dates, city or town, and five-digit zip codes.

Effective Date: **JUNE 24, 2021**

PATIENT RIGHTS – REQUESTS FOR RESTRICTIONS AND ALTERNATIVE MEANS OF COMMUNICATION – POLICY (7) AND PROCEDURE (7.1)

7. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.522.

7.1 **Procedure**:

a. **Individual Requests for Restrictions on the Use or Disclosure of PHI**
   i. Company will permit Individuals to request that Company restrict its uses and disclosures of PHI.
   ii. Company may refuse to honor Individual requests for restrictions on Company's use or disclosure of PHI.
   iii. Company employees, or those acting on Company's behalf, will forward Individual requests for restrictions to Company's Privacy Official.
   iv. Requests for restrictions will be received, processed and approved or denied by Company's Privacy Official, who will document the same in accordance with Policy 15.
   v. Company's Privacy Official will review all restriction requests and determine whether Company can reasonably accommodate the request.
   vi. **Agreeing to the Request**
      1. Company will honor requests for restrictions that it agrees to accept, except Company will not honor an Individual request for a restriction of disclosures of PHI to the Secretary of the Department of Health and Human Services.
      2. Company will agree to an Individual's request to restrict disclosure of PHI about the Individual to a health plan if:
         a. The disclosure is for the purpose of carrying out Payment or Health Care Operations and is not otherwise required by law; and
         b. The PHI pertains solely to a health care item or service for which the Individual, or person other than the health plan on behalf of the Individual, has paid Company in full.
      3. Company will take reasonable steps to ensure it abides by requests for restrictions it is required to or has agreed to honor.
   vii. **Denying the Request**
      1. If Company denies the request, Company will document the reason(s) for the denial.
      2. Company's Privacy Official will inform the Individual in writing of the denial and the reasons(s) for denial no more than ten (10) days after the determination, or as soon as reasonably possible.

viii. **Terminating the Restriction Agreement**

1. Company may terminate a request to restriction it has agreed to if:
    a. The Individual agrees to the termination in writing;
    b. The Individual orally agrees to the termination and the oral agreement is documented by Company; or
    c. Company informs the Individual it is terminating its agreement to the restriction (such termination is only effective with respect to the PHI created or received after Company has informed the Individual).

ix. **Emergency Situations**

1. In an emergency situation, Company may use or disclose Individual PHI that is subject to a restriction to a treatment provider for emergency treatment. Company will request that the provider not further use or disclose the information.

b. **Alternative Means of Communication**

i. Company will permit and, if reasonable, accommodate written requests by Individuals to receive communications of PHI from Company by alternative means or at an alternative location.

ii. Company's Privacy Official is responsible for determining whether an individual's request for a confidential communication is reasonable.

iii. Company may condition the provision of a reasonable accommodation on:
    1. When appropriate, information as to how payment, if any, will be handled; and
    2. Specification of an alternative address or other method of contact.

iv. Company may not require an explanation from the Individual as to the basis for the request as a condition of providing communications on a confidential basis.

v. If the Privacy Official determines that Company is unable to accommodate an Individual's request for receipt of PHI by alterative means or at an alternative location, the Privacy Official will document the basis for the determination and inform the Individual in writing within ten (10) business days of the determination, or as soon as reasonably possible.

Effective Date: **JUNE 24, 2021**

PATIENTS RIGHTS - ACCESS AND AMENDMENT OF PHI IN A DESIGNATED RECORD SET AND REQUESTS FOR AN ACCOUNTING OF DISCLOSURES – POLICY (8) AND PROCEDURE (8.1)

8. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.524, 45 CFR 164.526, 45 CFR 164.528, to the extent applicable.

8.1 **Procedure**:

a. **Individual Requests for Access to PHI**
   i. Unless otherwise described in this Procedure, Individuals have the right to access and obtain a copy of their PHI that is contained within a Designated Record Set maintained by Company for as long as the Designated Record Set is maintained by the Company.
      1. Company will permit and facilitate Individual access to such records in accordance with this Procedure.
   ii. Individuals do not have a right to access:
      1. Psychotherapy Notes; or
      2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
   iii. Company may require Individuals to pay a reasonable, cost-based fee (subject to limits imposed by other laws) for copying, postage, and preparation of the response to their access request.
   iv. Company will require Individuals to make requests for access to PHI in a Designated Record Set (e.g., Company's Breach reports to the Secretary, Breach notifications submitted to Individuals) in writing.
      1. Company will advise Individuals of this requirement in its Notice of Privacy of Practices.
   v. Company's Privacy Official, either personally or by delegation, will be responsible for receiving and processing requests for access and keeping a log of all requests and the deadline for the requested information. All documentation pertaining to requests of access and the Designated Record Sets that are subject to access by individuals shall be retained in accordance with Policy 15 below.
   vi. Company may only deny Individual requests for access to PHI in a Designated Record Set in accordance with this Procedure or as permitted by applicable state law.

b. **Access Granted**
   i. In the event that Company grants an Individual access to their PHI, it will:
      1. Ensure that access is provided to the Individual within thirty (30) days after receiving the request;
      2. If Company is unable to act on the access request within the initial thirty (30) day time period, it may extend the period by no more than thirty (30) days; provided that, within the initial thirty

(30) days, Company will provide the Individual with a written statement of the reasons for the delay and the date by which Company will provide a response to the Individual's access request; and

a. Company is only permitted to have one extension of time to act on an Individual's access request.

3. Company will provide the Individual with a copy of their PHI in the format agreed upon between the parties and will make PHI available in an electronic format if requested by the Individual.

c. **Access Denied – Review of Denial Permitted**

i. Company may deny an Individual access to PHI in their Designated Record Set if:

1. 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;
2. The PHI makes reference to another person (unless such other person is 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 such other person; or
3. The request for access is made by the 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.

ii. In the event that Company denies an Individual access for a reason listed in paragraph 8.1.c.i of this Procedure, Company will provide the Individual with the right to have the denial reviewed by a licensed health care professional who is designated by Company to act as a reviewing official and who did not participate in the original decision to deny.

iii. In addition to the requirements of paragraph 8.1.c.ii of this Procedure, in the event that Company denies the Individual's access request, it will, within the timeframes reflected in paragraph 8.1.b.i.2:

1. Provide the Individual with a timely explanation for the denial written in plain language that contains:
   a. The basis for the denial;
   b. A statement of the Individual's review rights and how the individual may obtain such review rights; and
   c. The process for complaining to Company or the Secretary of the Department of Health and Human Services.

iv. Individuals who wish to have a denial of access reviewed by a licensed health care professional will be referred to the Privacy Official.

1. The Privacy Official will identify and designate a licensed health care professional to perform the review.
2. The Privacy Official will forward the Individual's review request to the selected licensed health care official as soon as possible.
3. The selected licensed health care official will review the denial within a reasonable time period based and provide their decision in written form to Company.

d. **Access Denied – Review of Denial Not Permitted**
   i. Company may deny an Individual's request for access and not provide that Individual with the opportunity to request Company to review the decision in the following circumstances:
      1. The request is for Psychotherapy Notes;
      2. The PHI that is the subject of the request is compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding;
      3. When Company is acting under the direction of a correctional institution and the inmate's request would jeopardize the health, safety, custody or rehabilitation of the individual, other inmates or the safety of third parties;
      4. If the Individual has agreed to the denial of access when consenting to participate in research and Company informs the Individual that the right of access will be reinstated upon completion of the research; or
      5. If Company is not the source of the information and it received the information under the promise of confidentiality and access would be likely to reveal the confidential source.

e. **Summary Information**
   i. Company may provide an Individual with a summary or explanation of the PHI contained in their Designated Record Set (in lieu of access) if:
      1. The Individual agrees in advance to receive such a summary or explanation; and
      2. The Individual agrees in advance to any fees imposed by the Company.

f. **Individual Requests for Amendment of PHI**
   i. Unless otherwise described in this Procedure, Individuals have the right to request an amendment of their PHI that is contained within a Designated Record Set maintained by Company for as long as the Designated Record Set is maintained by the Company.
   ii. Individuals that request Company to amend their PHI must do so in writing and provide Company with a reason to support the requested amendment, provided that Company or the covered entity informed the Individual of the requirement that such request be made in writing.
   iii. Company will act on the Individual's request for an amendment no later than sixty (60) days after receipt of the Individual's written request.

1. If Company is unable to act on the amendment within sixty (60) days of the Individual's request, Company may extend the period by no more than thirty (30) days, provided that within the initial sixty (60) days, Company provides the Individual with a written statement for the delay and the date by which Company will complete its action on the Individual's request.
2. Company is only permitted to have one extension of time to act on an Individual's amendment request.

iv. Company's Privacy Official, either personally or by delegation, will be responsible for receiving and processing such requests and keeping a log of all requests and the deadline for the requested information. All documentation pertaining to requests for amendments shall be retained in accordance with Policy 15.

g. **Amendment Granted**

i. In instances when Company decides to make an amendment to PHI requested by an Individual, Company will:
1. Make the appropriate amendment to the PHI requested;
2. Identify the records in the Individual's Designated Record Set that are affected by the amendment and append or otherwise provide a link to the location of the amendment;
3. In accordance with the timeline reflected in paragraph 8.1.f.iii of this Procedure that Company accepted the Individual's request for amendment and obtain the Individual's agreement that Company can notify relevant persons or entities with which the amendment needs to be shared.
a. In the event that Company is able to obtain the Individual's agreement, Company will make reasonable efforts to inform and provide the amendment to relevant persons or entities identified by the Individual, including Business Associates who received PHI of the Individual and are in need of the amendment.

h. **Amendment Denied**

i. Company may deny an Individual's request to amend PHI in their Designated Record Set if it determines that the subject PHI:
1. Was not created by Company, unless the Individual provides Company with a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.
2. Is not part of Company's Designated Record Set;
3. The Individual would not have the right to access the information in accordance with this Procedure; and
4. Is accurate and complete.

ii. In the event that Company denies an Individual's request for an amendment for a reason listed in paragraph 8.1.h.i of this Procedure, it will, within the timeframes reflected in paragraph 8.1.f.iii:

1. Provide the Individual with a timely explanation for the denial written in plain language that contains:
    a. The basis for the denial;
    b. Information on how the Individual can file a written statement disagreeing with the denial and where it should be filed;
    c. A statement that if the Individual does not submit a statement of disagreement, the Individual may request that Company include the Individual's request for amendment and Company's denial of such with any future disclosures that Company makes of PHI that is the subject of the amendment; and
    d. A description of how the Individual may complain to Company or to the Secretary of the Department of Health and Human Services.
2. **Individual Statements of Disagreement**
    a. Company will permit Individuals to submit a written statement disagreeing with Company's denial of the requested amendment.
    b. Company may reasonably limit the length of the statement.
    c. Company may prepare a written rebuttal to an individual's written statement of disagreement and provide a copy of the same to the Individual.
        i. If Company prepares a rebuttal statement, it will provide the to the respective Individual.
    d. In instances where an Individual submits a written statement of disagreement, Company will:
        i. Identify the PHI that is the subject of the disputed amendment;
        ii. Append or otherwise link to the Individual's request for an amendment, Company's denial of the request, the Individual's statement of disagreement, and Company's rebuttal, if any; and
        iii. Include the material appended or a summary of the material with any subsequent disclosure of the PHI to which the disagreement relates.

i. **Notifications of Amendments from Other Covered Entities**
    i. If Company is informed by another covered entity of an amendment to an Individual's PHI, Company is responsible for amending the individual's PHI in accordance with the said amendment.

j. **Individual Requests for an Accounting of Disclosures**
    i. An Individual has a right to an accounting of disclosures made by Company and its Business Associates in the six years prior to the date of the request (the period may be shorter upon the Individual's request).

ii. Company will require an Individual to submit a request for an accounting of disclosures in writing.
iii. Company's Privacy Official will be responsible for receiving, processing, documenting and providing the request to the Individual.
iv. Company's Privacy Official will be responsible for tracking disclosures Company makes that are required to be included in an accounting. All documentation pertaining to requests for accounting of disclosures shall be retained in accordance with Policy 15.
v. With the exception of disclosures exempted from an accounting (as described in this Procedure), Company will provide an Individual with an accounting of disclosures within sixty (60) days of the Individual's request.
    1. In the event that Company is unable to provide an accounting within the initial sixty (60) day period, it may extend the period by no more than thirty (30) days, provided Company has given the Individual a written statement reflecting the reasons for the delay and the date by which Company will provide an accounting within the initial sixty (60) day period.
    2. Company may only have one extension of time to provide the Individual with an accounting of disclosures that has been properly requested.
vi. Disclosures listed on an Individual's accounting will not include the name of the workforce member(s) who accessed or disclosed the Individual's PHI.

k. **Disclosures Not Included in an Accounting**
    i. The following disclosures will be excluded from an Individual's accounting – those which are:
        1. To carry out Treatment, Payment, or Health Care Operations;
        2. To Individuals;
        3. Incident to a permitted or required use or disclosure;
        4. Made pursuant to an authorization;
        5. To persons involved in the Individual's care for notification purposes;
        6. Made for national security or intelligence purposes;
        7. To correctional institutions or law enforcement officials; and
        8. A part of a limited data set.

l. **Disclosures Included in an Accounting**
    i. The following disclosures will be included in an Individual's accounting – those which are:
        1. Required by law, including mandatory reporting to local, state, and federal agencies or authorities (e.g., immunization registries, animal bites);
        2. For public health activities (e.g., preventing/reporting disease, reporting vital events such as births and deaths, reporting child abuse, reporting communicable disease exposure, reporting adverse drug or vaccine reactions);

3. For victims of abuse, neglect, or domestic violence;
4. For health oversight activities (e.g., civil, administrative, or criminal proceedings);
5. For judicial and administrative proceedings (e.g., court orders, subpoenas);
6. For law enforcement purposes (e.g., regarding persons suspected to be a victim of a crime, reporting crime in emergencies);
7. To coroners, medical examiners, or funeral directors regarding decedent information;
8. For cadaveric organ, eye, and tissue donation;
9. For certain Research purposes;
10. To avert a serious threat to health or safety;
11. For specialized government functions, (e.g., military and veterans' activities, national security and intelligence activities);
12. For workers' compensation purposes; and
13. To a Business Associate for certain fundraising or marketing purposes.

m. **Content of the Accounting**

i. To the extent that Company is required to provide an Individual with an accounting of disclosures, such accounting will include the following:
   1. The Date of the disclosure;
   2. The Name of the entity or person who received the information and, if known, the address of the entity or person;
   3. A brief description of the PHI disclosed; and
   4. A brief statement of the purpose of the disclosure that briefly informs the Individual of the basis for the disclosure or a copy of the written request for such disclosure, if any.

ii. If there are multiple disclosures to the same person or entity for the same purpose, only the first disclosure needs to be documented in the format listed at paragraph 8.1.m.i (date, name, description, purpose). All other disclosures during the time period can be summarized by providing the following:
   1. The frequency, periodicity, or number of disclosures made during the accounting period; and
   2. The date of the last such disclosure during the accounting period.

iii. If there are multiple disclosures for a particular Research purpose for fifty (50) or more Individuals, the accounting may include:
   1. The name of the protocol or research activity;
   2. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
   3. A brief description of the type of PHI that was disclosed;
   4. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

5. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
6. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.
7. Company will assist the Individual in contacting the entity that sponsored the Research and the researcher requested by an Individual and if it is reasonably likely that Company disclosed the Individual's PHI in connection with Research.

n. **Suspension of Individual Right to an Accounting**

i. **Written Statements**

1. Company will temporarily suspend an Individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time period specified by the respective agency, if the such agency or official provide Company with a written statement that such an accounting to the Individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

ii. **Oral Statements**

1. To the extent the agency or the official submits a request to suspend an Individual's right to receive an accounting orally, Company will:
    a. Document the statement, including the identity of the agency or official making the statement;
    b. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
    c. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

o. **Fees for Providing an Accounting of Disclosures**

i. Company will provide the first accounting requested by an Individual in any 12-month period free of charge.
ii. Company may charge a reasonable, cost-based fee for subsequent accounting requests for an accounting made by the same Individual within the same 12-month period, provided:
    1. Company informs the Individual in advance of the fee; and
    2. Provides the Individual with a reasonable opportunity to withdraw or modify the request for a subsequent accounting in order to avoid the fee.

Effective Date: **JUNE 24, 2021**

COMPLAINTS AND PRIVACY INCIDENTS – POLICY (9) AND PROCEDURE (9.1)

9. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.530(d)(1)-(g)(1).

9.1 **Procedure**:

a. **In General**
   i. Individuals have the right to file complaints with the Privacy Official and/or with the Secretary.
   ii. Company's Privacy Official will be responsible for identifying, receiving, investigating, documenting, and responding to Individual complaints and privacy incidents concerning Individual PHI.
   iii. Company will direct workforce members and Business Associates, to forward all Individual complaints and privacy incidents concerning Individual PHI to Company's Privacy Official.
   iv. All Individual complaints and privacy incidents will be evaluated in accordance with Procedure 12.1.b.

b. **Individual Complaints**
   i. To the extent a complaint is received involving the use or disclosure of PHI, Company's Privacy Official will:
      1. Communicate with the complainant and advise them that the complaint is under investigation;
      2. Keep the complainant apprised of the status of the investigation to the extent appropriate;
      3. Document all communications with the complainant; and
      4. Document their activities in connection with the complaint, including their investigation, communications (both internally and externally), and mitigation efforts.

c. **Investigation**
   i. To the extent available, Company's Privacy Official will gather the following information in the course of their investigation into an Individual complaint or privacy incident involving Individual PHI:
      1. Description of the alleged incident, including a summary of the relevant facts;
      2. Identification of any electronic information systems or applications affected;
      3. The date the incident was discovered (i.e., the first day on which the complaint or privacy incident was known to Company (including a member of its workforce) or by exercising reasonable diligence would have been known;
      4. The date the complaint was made or the incident occurred;
      5. The number of Individuals affected;
      6. The type of PHI involved (e.g., demographic information, eligibility information, enrollment information);

7. The name of the complainant or the person that reported the incident;
8. Actions Company has taken in response to the complaint or incident; and
9. Any other relevant information.

ii. To the extent the complaint or privacy incident involves a Business Associate, the Privacy Official will review the relevant Business Associate Agreement to ensure Business Associate has and is complying with all obligations therein.

d. **Remediation Activities**

i. In connection with a substantiated Individual complaint or privacy incident, to the extent necessary, Company's Privacy and/or Security Official will:

1. Evaluate Company's administrative, technical, and physical safeguards to determine if such controls need to be adjusted;
2. Determine if Company's workforce members or its Business Associates need additional training;
3. Communicate and coordinate with external entities and/or law enforcement agencies (e.g., contacting the FBI in connection with a ransomware attack); and
4. Document all remediation activities.

e. **Sanctions**

i. For Individual complaints or privacy incidents resulting from, either in whole or in part, Company's workforce members or Company's Business Associates, Company's Privacy or Security Official will communicate and collaborate with appropriate Company personnel and recommend appropriate sanctions (e.g., consulting with Human Resources if a workforce member, business owner of relationship with Business Associate).

ii. Company's Privacy Official will ensure that appropriate sanctions are applied and documented in accordance with Policy 14 and Procedure 14.1.

f. **Refraining from Intimidating or Retaliatory Acts**

i. Company will not intimidate, threaten, coerce, or take any retaliatory acts against the Individual for filing a complaint with Company or with the Secretary (e.g., Company will not try to persuade an Individual to not file a complaint with Company).

ii. Company will not ask Individuals to waive their right to complain to the government or to Company.

iii. Company will not retaliate against persons who are not Individuals (e.g. Company workforce members) for participating in the complaint, investigation, or other process in connection with filing a complaint.

Effective Date: **JUNE 24, 2021**

BUSINESS ASSOCIATES AND BUSINESS ASSOCIATE AGREEMENTS – POLICY (10) AND PROCEDURE (10.1)

10. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.502(e)(1)-(e)(2), and 45 CFR 164.504(e)(1), to the extent applicable.

10.1 **Procedure**:

a. Company may delegate functions or activities to a Business Associate to the extent that the Company itself is permitted to use or disclose PHI under HIPAA.
b. Company will maintain a list of all Business Associate Agreements ("BAAs") it has executed.
c. Company, including its workforce members, will notify the Company Privacy Official in the event that it has reason to believe that a Business Associate has breached its BAA with Company.
d. Company's Privacy Official will be responsible for:
    i. Reviewing Company's list of BAAs no less than once annually to ensure it is accurate and complete;
    ii. Evaluating business relationships between external individuals and entities and Company and determining if a BAA is needed with the individual or entity;
    iii. Negotiating and executing written BAAs with individuals or entities that qualify as a Business Associate to Company (including the signing thereof);
    iv. Ensuring all HIPAA-required terms are present in executed BAAs;
    v. Ensuring that executed BAAs correspond and/or are connected to an executed services or other agreement with the in the individual or entity that qualifies as a Business Associate;
    vi. Mitigating and remediating breaches caused by Company's Business Associates; and
    vii. Assisting to determine whether or not Company can continue its relationship with a Business Associate in the event that Business Associate breaches its BAA with Company.
        1. If Company determines that the only way to mitigate the Business Associate's breach is to terminate the relationship with the Business, but that termination is not feasible, Company's Privacy Official will report the same to the Secretary.
e. If Company knows of a pattern of activity of a Business Associate that constitutes a material breach or violation of the Business Associate's obligations under its BAA with Company, Company will take reasonable steps to cure the breach or end the violation and if such steps are unsuccessful or not adequate, Company will terminate the BAA (if feasible) or report the violation to the Secretary or other enforcement agency, as needed and applicable.

Effective Date: **JUNE 24, 2021**

REASONABLE SAFEGUARDS FOR FAXING PHI – POLICY (11) AND PROCEDURE (11.1)

11. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.502(b) and 45 CFR 164.530 to the extent applicable; specifically, as it relates to faxing Individual PHI.

11.1 **Procedure**:

a. Prior to faxing Individual PHI, Company will determine if it is possible to disclose the subject PHI via another method (e.g., in an encrypted electronic format).
b. Company will limit its disclosure of Individual PHI via fax and will only transmit PHI via fax if necessary.
c. When transmitting PHI via fax, Company will:
    i. Verify the identity of the intended recipient and confirm his or her availability prior to sending the fax;
    ii. Verify the recipient's fax number;
    iii. Use a fax cover sheet that includes the following statement: "The information contained in this facsimile may be confidential and legally privileged. It is intended only for the use the of individual named. If you are not the intended recipient, you are hereby notified that the disclosure, copying, distribution or taking of any action in regards to the contents of this fax, except its direct delivery to the intended recipient is strictly prohibited. If you have received this fax in error, please notify the sender immediately and destroy this cover sheet along with its contents, and delete from your systems, if applicable;"
    iv. Send only the amount of PHI needed for the disclosure and/or to fulfill the request; and
    v. Verify the intended recipient received and secured the fax.
d. In the event that Company or a workforce member becomes aware that a fax has been misdirected, Company and/or the workforce member will attempt to retrieve or destroy the misdirected fax as well as notify Company's Privacy Official and provide the following information:
    i. The date the fax was sent;
    ii. The date it was discovered that the fax had been misdirected;
    iii. The person or entity that received the misdirected fax;
    iv. The type of information that was disclosed;
    v. How the error occurred; and
    vi. Information regarding attempts to retrieve and/or destroy the misdirected fax.

Effective Date: **JUNE 24, 2021**

BREACH NOTIFICATION - POLICY (12) AND PROCEDURE (12.1)

12. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.400 et seq. (aka the HIPAA Breach Notification Rule).

12.1 **Procedure**:

a. **General Responsibilities**
   i. Company's workforce members will be trained to identify and report all unauthorized uses and disclosures of Unsecured PHI to Company's Privacy Official.
   ii. Upon receiving notification or identifying an unauthorized use or disclosure of Unsecured PHI (including Individual complaints), Company's Privacy Official will conduct a risk assessment (in accordance with paragraph 12.1.b. of this Procedure) to determine whether or not the use or disclosure qualifies as a Breach.
   iii. Company will treat a Breach as discovered as of the first day on which such Breach is known by Company (or any employee, officer, or agent of Company), or, by exercising reasonable diligence, would have been known to Company (or any employee, officer or agent of Company).

b. **Risk Assessment**
   i. The risk assessment performed by Company's Privacy Official to determine whether or not an unauthorized use or disclosure of Unsecured PHI qualifies as a Breach, will include a review of the following:
      1. Whether the PHI used or disclosed was unusable, unreadable, or indecipherable prior to disclosure (e.g., was the PHI encrypted) thus rendering it secure. If not, continue;
      2. Whether the use or disclosure of PHI a violation of HIPAA (e.g., incidental disclosures are permitted and thus do not qualify as a violation. If yes, continue;
      3. Evaluating the probability that the PHI has been compromised by determining whether:
         a. The PHI disclosed alone, or in combination with other data, provides enough information for non-workforce member to identify or re-identify the Individual;
         b. The PHI disclosed involved data that is sensitive in nature (e.g., credit card numbers, social security card numbers, mental health, substance abuse, fertility information, etc.);

c. There is evidence that the PHI was actually acquired or viewed by a non-workforce member (the answer will be treated as "yes" if unknown);
d. The non-workforce member could have reasonably retained the information;
e. Who the recipient of the PHI was (e.g., a Business Associate, covered entity, member of workforce, an external individual who is unknown, an external individual who may use the information to harm the Individual); and
f. The recipient immediately returned or destroyed the PHI (and provided a written attestation to Company regarding the same).

ii. Company's Privacy Official will, after performing the risk assessment outlined above, determine whether or not the unauthorized use or disclosure of Unsecured PHI has resulted in a high or low probability of compromise;

iii. If the unauthorized use or disclosure of Unsecured PHI results in a low probability of compromise (i.e., not a Breach), Company's Privacy Official will document his or her analysis regarding the same; and

iv. If the unauthorized use or disclosure of Unsecured PHI results in a high probability of compromise (i.e., a Breach), Company's Privacy Official will document the same and notify all Individuals affected, the media (if required), and the Secretary in accordance with this Procedure.

c. **Internal and Individual Notification**

i. In the event that Company's Privacy Official determines a use or disclosure of PHI qualifies a Breach, the Privacy Official will:
1. Notify and collaborate with Company's legal counsel; and
2. Notify the affected Individual or Individuals of the Breach in writing without unreasonable delay, but in no event longer than sixty (60) calendar days after the date the Breach was discovered.

ii. **Requirements of the Written Notification to Affected Individuals**
1. The written notification to Individuals will be written in plain language and contain the following information:
a. A brief description of what happened, including the date of the Breach and date of discovery of breach, if known;
b. A general description of the types of PHI involved in the Breach (e.g. names, social security number, date of birth, home address, diagnosis, other medical related information);
c. Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
d. A brief description of what Company is doing to investigate the Breach, mitigate the harm and protect against any further Breaches; and

e. Contact information for individuals to ask questions or learn more information, which must include a toll-free number, an email address, website, or postal address.

iii. **Method of Notification to Individuals**

1. The written notification to Individuals will be sent via First Class Mail at the last known address of the Individual or, if the Individual agrees to electronic notice and such agreement has not been withdrawn, by secure electronic mail.
    a. In the event that Company knows that an affected Individual or Individuals is deceased and has the address of the Individual's next of kin or Personal Representative, Company will send written notification of the Breach to either the Individual's next of kin or Personal Representative.
    b. If the individual(s) affected by a breach is a minor(s) (a person under the age of 18 years) or lacks capacity due to a physical or mental condition, notice will be provided to the parent or person who is the personal representative of the individual.
2. In instances where there is insufficient or out-of-date contact information for ten (10) or more affected Individuals (as well as their next of kin or personal representative), Company will provide substitute notice to such affected Individuals by:
    a. Posting the notice in a prominent and conspicuous manner, for a period of ninety (90) days, on the home page of the website of Company or in major print or broadcast media in geographic areas where the Individuals affected by the Breach likely reside; and
    b. Include a toll-free phone number that remains active for at least ninety (90) days where an Individual can learn whether or not their PHI was affected by the Breach.
3. In instances where there is insufficient or out-of-date contact information for fewer than ten (10) affected Individuals (as well as their next of kin or personal representative), Company may provide substitute notice to such affected Individuals via alternative form of written notice, telephone number, or other means.
4. In instances deemed by Company to require urgency because of possible imminent misuse of Unsecured PHI, Company may provide information to affected Individuals by telephone or other means, as appropriate, in addition to the notice required by paragraph 12.1.c.iii.1 of this Procedure.

iv. **Notification to the Secretary and the Media**

1. **Breaches involving fewer than five hundred (500) Individuals**

a. Company's Privacy Official will, not later than sixty (60) days after the end of each calendar year, notify the Secretary (electronically, via and in accordance with the HHS Office for Civil Rights' website) of all Breaches Company has experienced that involve fewer than five hundred (500) Individuals.

2. **Breaches involving five hundred (500) or more Individuals**
   a. Company's Privacy Official will, not later than sixty (60) days after the Breach is discovered notify the Secretary (electronically, via and in accordance with the HHS Office for Civil Rights' website).
   b. Company will notify a local media outlet without unreasonable delay but no later than sixty (60) days after the date of discovery of the Breach.
   c. Company will place a notification of the Breach in a conspicuous location on Company's website and leave the notification up for at least ninety (90) days.
   d. The content of the "media" notification as well as the notification posted to Company's website will include the information described in paragraph 12.1.c.ii of this Procedure.

v. **Law Enforcement Delay**
   1. Notifications required and described in this Procedure may be delayed if a law enforcement official provides a written or oral statement that such notification would impede a criminal investigation or cause damage to national security.
   2. Company's Privacy Official will confirm that the written statement by the law enforcement official specifies the time for which a delay is required.
      a. If the statement is made orally, Company's Privacy Official will document the statement, including the identity of the official making the statement, and delay the notification for no longer than thirty (30) days (unless a written statement is submitting during the thirty (30) day period.

vi. **Mitigation**
   1. Company will mitigate, to the extent practicable, any harmful effect that is known to Company of a use or disclosure of PHI in violation of the Company's HIPAA policies or procedures by the Company, its employees or workforce members, or a Business Associate of Company.

vii. **Breaches Caused by Business Associates**
   1. Company will (in its respective Business Associate Agreements) require its Business Associates to notify Company of Breaches caused by a Business Associate to Company without unreasonable delay and no later than sixty (60) days from the

discovery of the Breach (Company may require a shorter reporting time frame as set forth in its Business Associate Agreement).

2. Company will further require, to the extent possible, the Business Associate to provide Company with the identification of each Individual affected by the Breach as well as any information required by Company in order to provide notification to affected Individuals and the Secretary.

viii. **Accounting of Disclosures**

1. All unauthorized disclosures of information, regardless of whether they are ultimately determined to constitute a Breach after conducting the risk assessment discussed in paragraph 12.1.b of this Procedure, must be documented in the Individual's accounting of disclosures.

Effective Date: **JUNE 24, 2021**

WORKFORCE PATIENT HIPAA EDUCATION AND TRAINING - POLICY (13) AND PROCEDURE (13.1)

13. **Policy**: It is the policy of Company ("Company") to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.530(b).

13.1 **Procedure**:

a. Company's Privacy Official will develop privacy and security education and training and will provide the same to Company's workforce members, as needed and as appropriate given the workforce member's job responsibilities in relation to PHI.
b. Company's Privacy Official will ensure that new workforce members are provided with privacy and security training, including training on the requirements and standards reflected in Company's HIPAA Privacy and Security Policies and Procedures, during Company's new-hire orientation process or as otherwise appropriate.
c. Company's Privacy Official will ensure that newly hired workforce members and/or workforce members that have been transferred or re-assigned, receiving the training referred in paragraph 13.1(a) of this Procedure within thirty (30) days of such hire, transfer, or re-assignment, as needed and as appropriate.
d. Company's Privacy Official will ensure that on-going educational awareness and training occur at least once annually and as needed to the extent Company makes a material change to a HIPAA privacy or security policy or procedure.
e. Company's Privacy Official will determine if a workforce member requires additional, unique, or specialized training as it relates to the responsibilities in relation to Company's use or disclosure of PHI.
f. The Privacy Official will ensure that documentation is maintained supporting workforce members' educational awareness and training (e.g., a certificate indicating training has been successfully completed) in accordance with Policy 15.

Effective Date: **JUNE 24, 2021**

SANCTIONS - POLICY (14) AND PROCEDURE (14.1)

14. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.530(e).

14.1 **Procedure**:

a. Violations of Company's HIPAA Privacy or Security Policies and Procedures will be reported to Company's Privacy Official.
b. Company's Privacy Official will investigate all reported or discovered violations in a timely manner.
c. Company's Privacy Official will report all confirmed violations of Company's HIPAA Privacy or Security Policies and Procedures to Company's Human Resources department.
    i. Workforce members that violate Company's HIPAA Privacy or Security Policies and Procedures be subject to disciplinary action up to and including termination, as determined by Company in conjunction with its Human Resource's department and legal counsel.
        1. The types of sanctions that may imposed include, but will not be limited to the following: verbal warning, written reprimand, re-training, suspension, termination, and/or reports to authorities (state and/or federal). This Procedure does not alter the at-will status of any Company employee/workforce member.
d. Company will not impose sanctions against any employee or workforce member for: (i) engaging in whistleblower activities, including to the extent that such activities involve the disclosure of PHI to the extent permitted under 45 CFR 164.502(j); (ii) submitting a complaint to the Secretary or testifying, assisting, or participating in an investigation, compliance review, or hearing as set forth in 45 CFR 160.316; or (iii) opposing any act or practice made unlawful under HIPAA, provided that the employee or workforce member has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule
e. Company shall retain documentation regarding any sanction imposed for a violation of Company's HIPAA Privacy or Security Policies and Procedures in accordance with Policy 15.
    i. Copies of the documentation, including documentation relating to the sanctions imposed by the Company against its Business Associates should be forwarded to the Company's Privacy Official and maintained for the same retention period.

Effective Date: **JUNE 24, 2021**

RETENTION OF DOCUMENTATION – POLICY (15) AND PROCEDURE (15.1)

15. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding 45 CFR 164.530(j).

15.1 **Procedure**:

a. Company will maintain the documentation identified below for a period of no less than six (6) years from the date in which it was created and/or the date when it was last in effect, whichever is later:
    i. Company's HIPAA Privacy Policies and Procedures;
    ii. Company's HIPAA Security Policies and Procedures;
    iii. Any communication Company is required to make in writing in accordance with its HIPAA Privacy or Security Procedures, or that is otherwise required by HIPAA. (e.g., Company's Breach reports to the Secretary, Breach notifications submitted to Individuals);
    iv. Any action, activity, or designation Company is required to make pursuant to its HIPAA Privacy or Security Procedures, or that is otherwise required by HIPAA. (e.g., designation of Company's Privacy Official, fulfilling an Individual's request for access to his or her Designated Record Set); and
    v. All other documentation that Company is required to create and maintain in accordance with its HIPAA Privacy or Security Procedures, or that is otherwise required by HIPAA (e.g., Company's Notice of Privacy Practices, risk assessment documentation, etc.).
b. Company shall make the documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
c. Company shall review documentation periodically, and update documentation as needed, in response to environmental or operational changes affecting the security of electronic PHI.

Effective Date: **JUNE 24, 2021**