The Children's TherAplay Foundation, Inc. ("Covered Entity")

PROTECTED HEALTH INFORMATION PRIVACY AND SECURITY POLICIES

Effective Date: October 18, 2021

Prepared by:

Krieg DeVault LLP

KD_13336154_1

PROTECTED HEALTH INFORMATION PRIVACY AND SECURITY POLICIES

TABLE OF CONTENTS

ARTICLE I - ADMINISTRATION 1

A. Information Security Risk Assessment and Management. 1
B. Privacy/Security Officer 1
C. Screening and Clearance 1
D. Training and Monitoring 2
E. Complaints and Incidents 2
F. Investigation; Enforcement 2
G. Written Notification of Breach 2
H. Contingency Plan; Mitigation 2
I. Sanctions 3
J. Policy Related Documents 4
K. Patient-Specific HIPAA Documents 4
L. No Retaliatory Acts 4

ARTICLE II - HOW COVERED ENTITY WILL CREATE AND MAINTAIN PROTECTED HEALTH INFORMATION 4

A. Protected Health Information. 5
B. De-Identified Health Information; Deceased Patients. 5
C. Retention of PHI and Related Forms 6

ARTICLE III - HOW COVERED ENTITY WILL USE AND DISCLOSE PROTECTED HEALTH INFORMATION 6

A. To Provide Treatment, Obtain Payment, and Perform Certain Health Care Operations. 6
B. Pursuant to Certain Laws That "Require" Disclosure by Covered Entity Without An Executed Authorization Form 9
C. Pursuant to Certain Laws That "Permit" Disclosure by Covered Entity Without An Executed Authorization Form 10
D. Pursuant To An Executed Authorization Form. 13
E. Validation Procedure for Disclosures of PHI and ePHI Contrary to This Policy 13
F. Prohibition on Sale of PHI 13

ARTICLE IV - HOW COVERED ENTITY WILL MANAGE PATIENTS' INDIVIDUAL RIGHTS REGARDING THEIR PROTECTED HEALTH INFORMATION 14

A. Right to Notice of Privacy Practices. 14
B. Right to Request Certain Restrictions on PHI Uses and Disclosures. 14
C. Right to Request Access to PHI. 15
D. Right to Request Amendment of PHI. 17
E. Right to an Accounting of PHI Disclosures. 18

F. Right to Notification of Breach Involving Unsecured PHI or Other Unauthorized Access to Personal Information. 19
G. Right to Contact Privacy/Security Officer and File a Complaint. 19

ARTICLE V - HOW COVERED ENTITY WILL MANAGE CONTRACTUAL RELATIONSHIPS WITH BUSINESS ASSOCIATE RELATIONSHIPS 19

A. Roster; Agreement or Addendum 19
B. Vendors and Other "Business Visitors" 19

ARTICLE VI - HOW COVERED ENTITY WILL SAFEGUARD PROTECTED HEALTH INFORMATION FROM UNAUTHORIZED ACCESS 19

A. Access Controls. 20
B. Workforce Controls. 20
C. Electronic Media Controls. 21
D. Communication Controls. 22
E. Electronic Communication Controls 22

ARTICLE VII - GLOSSARY OF TERMS 24

Attachment 1 - Potential Privacy Laws 31

Attachment 2 - HIPAA Privacy/Security Training Handout 32

Attachment 3 - HIPAA Training Certification Form 37

Attachment 4 - Workforce Confidentiality Agreement 38

Attachment 5 - Action Form 41

Attachment 6 - Privacy/Security Flow Sheet 42

Attachment 7 - HIPAA Risk Assessment Form 43

Attachment 8 - Decision Tree in Order to Determine any HIPAA Breach Notification Obligations 44

Attachment 9 - Notification Requirements Under Indiana Law for an Unauthorized Access to Personal Information 48

Attachment 10 - HIPAA and State Law Requirements Governing Patient Notifications in the Case of a HIPAA Breach or other Unauthorized Access to Personal Information Governed by State Law 50

Attachment 11 - Patient Request to Restrict PHI Uses and Disclosures Form 52

Attachment 12 - Authorization for the Disclosure of Protected Health Information on Social Media 54

Attachment 13 - Authorization for the Disclosure of Protected Health Information.....56

Attachment 14 - Notice of Privacy Practices 58

Attachment 15 - Acknowledge of Notice of Privacy Practice 59

Attachment 16 - Patient Request to Access PHI Form.....60

Attachment 17 - Patient Request to Amend PHI Form.....62

Attachment 18 - Patient Request for Accounting of PHI Disclosures Form 65

PROTECTED HEALTH INFORMATION
PRIVACY AND SECURITY POLICIES

PREAMBLE

The Children's TherAplay Foundation, Inc. ("Covered Entity") has adopted these Protected Health Information Privacy and Security Policies ("Policies") in order to safeguard the privacy and security of all Protected Health Information and Personal Information (collectively "PHI") that is part of the Patient Record maintained by Covered Entity, in accordance with applicable laws and regulations. These Policies assume that all Patients treated by the Covered Entity are minor Patients and that the Personal Representative will have authority to control the health care and Patient Record of the Patient.

All capitalized terms not otherwise defined within the text of these Policies are set forth in Article VIII, "Glossary of Terms." Covered Entity may consult the federal and state privacy laws on **Attachment 1**, as may be applicable, while providing services to its patients and if questions should arise that are not addressed in these Policies.

ARTICLE I
ADMINISTRATION

A. **Information Security Risk Assessment and Management**. Covered Entity or it designee will perform a HIPAA security risk analysis and assessment and will update on a regular basis, a HIPAA

B. **Privacy/Security Officer**. Covered Entity's policies shall be overseen by a Privacy and Security Officer(s) for Covered Entity with the following responsibilities:

1. Oversee the development and implementation of these Policies as they pertain to PHI generally by all Workforce.

2. Review and approve, as appropriate, certain procedures and forms governing PHI privacy and security that are described in these Policies.

3. Serve as the primary contact person for all Complaints, Security Incidents, and questions concerning PHI privacy and security and Covered Entity's compliance with these Policies.

4. Monitor and audit all Workforce compliance with these Policies and related services, systems, and operations in order to detect, mitigate, and correct any behavior or events that may result in a violation of these Policies.

5. Report to Covered Entity's legal counsel, Executive Director and Board of Directors on these matters as appropriate.

C. **Screening and Clearance**. Covered Entity shall screen all Workforce, in accordance with Covered Entity policies and procedures, in order to confirm the qualifications and trustworthiness

of all Workforce who may access Covered Entity's physical premises, Electronic Media, and PHI for Treatment, Payment, or Health Care Operation purposes.

D. **Training and Monitoring**. Covered Entity shall arrange for all Workforce to attend Covered Entity's mandatory HIPAA training program, at least annually. Covered Entity shall also arrange for all new Workforce to attend Covered Entity's then-current mandatory HIPAA training program. Attachment 2 or alternative training documents, may be used for by Covered Entity for Workforce training. The Privacy/Security Officer shall ensure that attendance is documented and obtain Workforce certifications of attendance and compliance (Attachment 3). The Privacy/Security Officer should also have all Workforce sign a Workforce Confidentiality Agreement (Attachment 4). Covered Entity shall conduct, document, and report all regular, and if necessary, special procedures that are conducted by the Privacy/Security Officer, or designee, for the purpose of monitoring and auditing Workforce compliance with these Policies and to review Covered Entity's information system activity.

E. **Complaints and Incidents**. All Workforce have an affirmative duty to notify the appropriate Privacy/Security Officer(s) and submit a completed Action Form (**Attachment 5**) if there is reason to believe that any member of the Workforce, Business Associate, or other third party may have violated any of these Policies resulting in a Complaint, a Successful Security Incident, a Breach, or other Unauthorized Access to PHI (hereinafter collectively referred to as "Incident"). All Patients of Covered Entity are similarly advised in the Notice of Privacy Practices to inform the Privacy/Security Officer of any Complaints at any time. All reported Complaints and Incidents are documented by the Privacy/Security Officer. Any Disclosure of PHI (other than for Treatment, Payment, or Health Care Operations, as may be requested by the Patient's Personal Representative, or Incidental Uses and Disclosures) shall also be logged in the affected Patient's HIPAA Privacy/Security Flow Sheet (**Attachment 6**), as described in more detail in Article 4(E).

F. **Investigation; Enforcement**. The Privacy/Security Officer, in conjunction with Covered Entity's designated legal counsel if requested by the Privacy/Security Officer, shall investigate any and all Incidents. In conjunction with any investigation, the Privacy/Security Officer shall complete the HIPAA Risk Assessment form and maintain in the investigation file. (**Attachment 7**) and may also review the Decision Tree (**Attachment 8**). Any resulting disciplinary or corrective action shall be carried out by the Human Resources Director or other Covered Entity leadership as appropriate in accordance with applicable Covered Entity policies and procedures. If any investigation involves a Business Associate, the appropriate member of Covered Entity's administrative team will be included in the investigation and receive a copy of the report. The Privacy/Security Officer shall maintain a complete and confidential investigation file for all Complaints and Incidents, regardless of the outcome of the investigation.

G. **Written Notification of Breach**. As soon as possible upon confirming any Incident, the Privacy/Security Officer, in conjunction with designated legal counsel, shall complete all Patient, state and federal notifications required under HIPAA or applicable state laws, without unreasonable delay, but no later than sixty (60) days after Covered Entity discovers the Incident. **Attachments 9 and 10** provide additional information about breach notification requirements.

H. **Contingency Plan; Mitigation**. Covered Entity has or will establish promptly after the Effective Date of these Policies a contingency plan that permits Covered Entity to promptly detect,

mitigate, and correct, to the extent practicable, any Incident. The plan will include performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. All actions taken by Covered Entity responsive to an Incident shall be documented by the Privacy/Security Officer.

I. **Sanctions**. The Human Resources Director, in conjunction with the Privacy/Security Officer, will maintain, consistently impose, and document appropriate sanctions against all Workforce who violate HIPAA and/or this Policy to be administered as follows:

1. **Level 1: Careless Violation**.

   a. This violation occurs when a Workforce member unintentionally or carelessly gains Access (as defined) to PHI.

   b. Examples may include: (a) PHI is accidentally communicated by a Workforce member acting within the scope of his/her employment to a person who has no reason to Access the PHI, whether by telephone, regular mail, fax, or otherwise; and (b) PHI is accidentally left unattended in a public area that may be accessible by persons who have no reason to Access the PHI.

   c. Disciplinary sanctions for this violation will be administered in a progressive manner. First and all subsequent offenses, depending upon the facts and circumstances, may include counseling, oral warning, written warning, final written warning, suspension, or termination, all of which shall be documented by the Human Resources Department and the Privacy/Security Officer.

2. **Level 2: Knowing Violation**.

   a. This violation occurs when a Workforce member knew or should have known that his/her actions or inactions would result in an unauthorized Access (as defined) to PHI or Workforce otherwise disregards this Policy resulting in a HIPAA violation.

   b. Examples may include: (a) discussing PHI in a public area or local restaurant; (b) failing to destroy and/or dispose of PHI properly; (c) failing to lock personal vehicle resulting in a theft of PHI or Electronic Media containing PHI that is left in the vehicle; (d) failing to encrypt an e-mail communication containing PHI that is transmitted to an individual that is not otherwise conducted within Covered Entity's intranet firewall; (e) any Access to PHI without a Legitimate Need to Know (e.g., looking up your the PHI of a Patient because you are curious or because the Patient is a child of a famous person); and (f) posting Patient information on an Internet social networking website (e.g., Facebook, Twitter) regardless of whether the posting was made while on duty or not unless the Covered Entity has obtained an Authorization in compliance with HIPAA, all other related requirements of this Policy, and Covered Entity's Social Media Policy.

c. Disciplinary sanctions for this violation shall include either suspension of up to three (3) days from work without pay or termination of employment, depending upon the facts and circumstances, all of which shall be documented by the Human Resources Department and the Privacy/Security Officer.

3. **Level 3: Intentional Violation**.

a. This violation occurs when a Workforce member intentionally or recklessly disregards these Policies, which results in a serious violation of HIPAA.

b. Examples may include: (i) a Workforce member's failure to report a known or suspected Incident to the Privacy/Security Officer; (ii) a Workforce member's Access to PHI to steal a Patient's identity; (iii) gaining Access to PHI which is sold to a third party; and (iv) gaining Access to PHI for other unlawful, unethical, or other unprofessional purposes.

c. Disciplinary sanctions for this violation are immediate termination of employment, which shall be documented by the Human Resources Department and the Privacy/Security Officer.

J. Policy Related Documents. Covered Entity, and its Business Associates, will maintain a copy of all current and previously adopted HIPAA policies and procedures, risk assessment work papers, reports, forms, attachments, and other related documentation related to this Policy. A copy of all such documents shall be maintained by the Privacy/Security Officer for at least seven (7) years from the date of the document's creation or the date when the document was last in effect, whichever is later.

K. Patient-Specific HIPAA Documents. All Patient-specific HIPAA forms, attachments, and other related documentation created or received by Covered Entity as part of the implementation of this Policy shall be maintained in a privacy file of the applicable Patient Record for at least seven (7) years. Examples include signed Patient Acknowledgment Forms, subpoenas and third-party requests, and completed copies of Patient requests pursuant to this Policy, among others.

L. No Retaliatory Acts. Covered Entity will not tolerate any act by Workforce to intimidate, threaten, coerce, retaliate, or discriminate against any Patient or other person who (1) exercises an individual Patient right recognized by these Policies, or (2) files a Complaint or reports a Security Incident with, or testifies, assists, or participates in an investigation, compliance review, proceeding, or other administrative or enforcement action conducted by, the Office for Civil Rights or other governmental agency, which concerns Covered Entity's compliance with these Policies or other applicable laws and regulations.

ARTICLE II
HOW COVERED ENTITY WILL CREATE AND MAINTAIN PROTECTED HEALTH INFORMATION

A. Protected Health Information.

1. **Patient Record**.

   a. Covered Entity shall create, label, and maintain an electronic Patient Record that complies with all record-keeping requirements necessary for treatment and billing purposes. NOTE: No Personal Information (e.g., SSN) shall be used to label a particular Patient Record.

   b. The Patient Record does not include the following information that may be received, created, or used by Covered Entity from time to time: (i) administrative data (e.g., completed forms and other documents created under these Policies and filed in the Patient Record under the Privacy Tab, including the Flow Sheet (**Attachment 6**); and, (ii) quality improvement data, Complaint, and/or Incident reports, Action Forms. Any such material may be retained by Covered Entity in a separate database, folder, or otherwise, but shall not be considered part of the Patient Record at any time. The Patient Record represents the entire PHI of the Patient that is subject to these Policies.

2. **Authorized Users**. Covered Entity shall designate all members of the Workforce who are authorized to access PHI in any manner and any applicable "minimum necessary" standards that may apply. These Minimum Necessary Standards do not apply to: (i) Disclosures, and any requests for PHI, made by Covered Entity to other health care providers who maintain a treatment relationship with the Patient for Treatment and Payment; (ii) Disclosures to the Patient; (iii) Disclosures pursuant to an Authorization; (iv) Disclosures or uses required for compliance with HIPAA simplification rules; (v) Disclosures to the Department of Health and Human Services when disclosure is required for enforcement purposes; or (vi) Disclosures or uses required by other state and federal laws.

B. De-Identified Health Information; Deceased Patients.

1. **Not Subject to Policies.** Health Information which has been De-Identified is no longer considered PHI and does not in any way identify a Patient in accordance with the Regulations, including but not limited to: 45 C.F.R. § 164.502(d), and implementation specifications in 45 C.F.R. § 164.514(a)-(b), and with respect to which there is no reasonable basis to believe that the remaining information can be used, alone or in combination with other information, to identify a Patient, and therefore does not qualify as PHI subject to these Policies. Any Health Information that is to qualify as De-Identified Health Information must be reviewed and verified by the Privacy/Security Officer before it leaves Covered Entity's premises, including documentation as to the method of de-identification, whether by expert or by removal of specified individual identifiers.

2. **Re-Identified Health Information Subject to Policies**. Any De-Identified Health Information that is later Re-Identified for any reason, such as by disclosure of a

code or other means of record identification designed to enable coded or otherwise De-Identified information to be Re-Identified, constitutes disclosure of PHI and shall only be Used or Disclosed by Covered Entity in accordance with the Policies governing Uses and Disclosures of PHI set forth in these Policies.

3. **Deceased Patients**. Covered Entity may Disclose a Deceased Patient's PHI to family members and others involved in the Deceased Patient's Treatment or Payment prior to death, but only to the extent that the family was involved in the particular Treatment or Payment functions, and only to the extent Covered Entity is not aware of any prior expressed restriction of the Patient or Personal Representative known to Covered Entity.

C. Retention of PHI and Related Forms. All Records of minor Patients shall be retained for no less than seven (7) years following the last date that the subject Patient received services from Covered Entity. Covered Entity should also review all requirements of applicable payors for record retention. Irrespective of the above rules, Patient Records that are the subject of any pending litigation or other claim shall be retained pursuant to the prior express written instructions of an authorized representative of Covered Entity and its legal counsel.

ARTICLE III
HOW COVERED ENTITY WILL USE AND DISCLOSE PROTECTED HEALTH INFORMATION

A. To Provide Treatment, Obtain Payment, and Perform Certain Health Care Operations. Covered Entity may Use or Disclose PHI to carry out Treatment, Payment, or Health Care Operations, or to assist another Covered Entity in its efforts to carry out Treatment or Payment functions, without an executed Authorization Form, but if the Disclosure is to be made to another Covered Entity for Health Care Operations of the other Covered Entity, then the Disclosure shall only be permitted after the Privacy/Security Officer has independently verified that Covered Entity and the other Covered Entity both have a relationship with the Patient.

1. **Personal Representatives (Parents/Legal Guardians) Involved in a Patient's Treatment or Payment**. Covered Entity may Disclose PHI to a Personal Representative, which includes the parents and legal guardian, of a minor Patient. This includes disclosure to a custodial parent of a child and a noncustodial parent of a child unless the Covered Entity has a copy of a court issued order that limits the noncustodial parent's access to the child's health record or the Covered Entity has actual knowledge of that record. The Covered Entity may only disclose PHI to another person that is not a Personal Representative, such as a babysitter, if the Personal Representative has signed an Authorization. The Covered Entity should request upon new Patient intake that the Personal Representative designate any other individuals that will be attending therapy with the Patient and ask the Personal Representative to sign an Authorization if that individual will be present during therapy sessions or otherwise need access to Patient PHI. In addition, even when the Patient's Personal Representative is absent, incapacitated, or it is otherwise impracticable to obtain a Personal Representative's consent in an emergency, a Disclosure to another individual accompanying the Patient is permitted when, in

exercising professional judgment, it determines that doing so would be in the best interest of the Patient.

2. **Special PHI Rules**. Any Uses and Disclosures of a Patient's PHI for Treatment, Payment, or Health Care Operations shall be subject to the special rules for Mental Health Records, Drug and Alcohol Treatment Records, and Communicable Disease Records. Should Covered Entity ever create or obtain these types of special records, it should immediately notify the Privacy Officer/Security Officer for further instructions.

3. **Approved Personal Representative Restrictions**. Any Uses and Disclosures of a Patient's PHI for Treatment, Payment, or Health Care Operations shall be subject to any requested restrictions by the Personal Representative that are approved and documented by the Privacy/Security Officer, except if emergency care is required. (**Attachment 11)**

4. **Minimum Necessary Standards**. Covered Entity has designated the Minimum Necessary standards that will limit certain Uses and Disclosures of PHI and ePHI for Treatment, Payment, and Health Care Operations by Workforce, based upon a Need to Know standard, in order to accomplish the intended purpose. The Minimum Necessary Standards do not apply to: (a) Any Uses or Disclosures where a Limited Data Set would be sufficient to accomplish the purpose of a particular PHI request, Use, or Disclosure, as determined by the Privacy/Security Officer (or designee); (b) Disclosures and any requests for PHI made by or between Covered Entity to other health care providers who maintain a business relationship with the Patient for Treatment and Payment purposes; (c) Disclosures to the Patient or their Personal Representative; (d) Disclosures required by law; (e) Disclosures pursuant to an Authorization; or (f) Treatment of a Patient in an emergency.

5. **Incidental Uses/Disclosures**. HIPAA is not intended to hinder customary and necessary Health Care communications by Covered Entity. As a result, Covered Entity permits certain Incidental Uses and Disclosures of PHI that may occur, but only to the extent that reasonable safeguards (e.g., communications conducted in non-public areas or in public areas using low voice tones that are not audible to unauthorized third parties, to the extent possible) are used to limit Uses and Disclosures and the Minimum Necessary Standards are satisfied. Examples of permitted Incidental Uses/Disclosures includes communications conducted in the lobby with Personal Representatives of Patients to the extent low voices are used that are not audible to third parties, or communications and interactions in the horse arena while other Patients or their Personal Representatives are present so long as Workforce make an effort to not disclose specifics of therapy treatment to other Patients or Personal Representatives.

6. **Interpreters**. Covered Entity shall use an Interpreter to communicate with a Patient, to the extent required by law; however, Authorization signed by the Patient is not required if an Interpreter is used and each of the following conditions is met:

a. The communication is related to Treatment, Payment, or Health Care Operations; and

b. The communication involves a Patient who speaks a language other than English or who is hearing impaired or hard of hearing.

For purposes of this Policy, a qualified Interpreter means a member of the Workforce, Business Associate or a family member, close friend, or other person designated by the Patient to serve as his/her Interpreter.

7. **Research.** Any questions or requests for PHI for research purposes shall be sent directly to the Privacy Officer or his or her designee. The Privacy Officer shall work with legal counsel on any such research requests.

8. **Marketing**. HIPAA gives individuals control over whether and how their PHI is used and disclosed for marketing purposes by requiring a Patient's or their Personal Representative's written authorization, as applicable, before Use or Disclosure of his/her PHI can be made for marketing. Marketing may occur when a communication is made that encourages recipients of the communication to purchase or use a product or when PHI is sold to another entity for purposes of that entity marketing to those individuals. Such Disclosures for marketing purposes shall not occur without first receiving the Patient's or Personal Representative's consent.

   Patient or Personal Representative authorizations are not required when communications are made for reasons related to patient care or to promote the covered entity's own products and services. Examples include: discussing care management and care coordination; communicating the covered entity's new services to a Patient. The Privacy/Security Officer shall approve marketing initiatives to ensure they meet the requirements of this policy, HIPAA rules (45 C.F.R. § 164.501 and 508(a)(3)), and Office for Civil Rights guidance regarding marketing.

9. **Public Relations and Social Media**. All such requests for disclosure of any PHI to a television, radio, or newspaper must be directed to and approved by the Privacy/Security Officer or their designee. The Privacy/Security Officer shall only allow for the disclosure of such PHI to a television, radio, or newspaper after first obtaining an Authorization signed by the Personal Representative and complying with Covered Entity's Social Media Policy. Likewise, only a representative designated by the Privacy/Security Officer may post any PHI on the Covered Entity's Social Media and only after the Personal Representative has signed the Authorization for Disclosure of Protected Health Information on Social Media (**Attachment 12**).

10. **Psychotherapy Notes**. No Covered Entity representative shall disclose any Psychotherapy Notes pertaining to a particular Patient, unless the subject Patient has signed a written authorization. However, no authorization is required to carry

out certain operations involving the use of the psychotherapy notes, including use by the health care provider who created the notes for treatment of a Patient, use by Covered Entity for its own training programs in mental health, or Use or Disclosure required to defend Covered Entity in the instance of a legal proceeding brought by the Patient, and such other uses pursuant to the HIPAA regulations.

B. Pursuant to Certain Laws That "Require" Disclosure by Covered Entity Without An Executed Authorization Form. As directed by the Privacy/Security Officer, who shall first verify any applicable special rules for Mental Health Records, Drug and Alcohol Treatment Records, and Communicable Disease Records, and even without an executed Authorization Form, Covered Entity is required to Disclose a Patient's PHI in any of the following circumstances:

1. **Department of Health and Human Services**. Covered Entity shall Disclose PHI to the Secretary of the Department of Health and Human Services ("HHS") solely for purposes of investigating or determining compliance with HIPAA.

2. **Public Health Reporting**. Covered Entity shall Disclose PHI, not including Mental Health Records, Drug and Alcohol Treatment Records, and Communicable Disease Records except as set forth herein, to a public health authority that is authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability, which includes reporting disease, injury, vital events such as birth or death, public health surveillance or investigations, and public health interventions, and in particular, reports made pursuant to Indiana and federal laws regarding the following: (i) Blindness and Visual Impairment, I.C. §14-40-2-1; (ii) Communicable Diseases, I.C §16-41-2-2 and 410 IAC §1-2.1-2; (iii) Deaths Related to Blood Transfusions, 21 CFR §606.170(b); (iv) Deaths Due to Unnatural Causes, I.C. §16-37-3-7; (v) Treatment of Persons with Disabilities, I.C. §16-40-1-1 et seq.; and (vi) Tuberculosis, 410 IAC §1-2.1-2;

3. **FDA**. Covered Entity shall Disclose PHI to a person subject to the jurisdiction of the FDA for the following purposes: (i) to report adverse events or product defects or deviations, if the Disclosure is made to the person required or directed to report the information to the FDA; (ii) to track products, if the Disclosure is made to the person required or directed by the FDA to track the product; (iii) to enable product recalls, repairs, or replacement (including locating and notifying Patients who received the product); or (iv) to conduct post-marketing surveillance to comply with FDA requirements, provided that Drug and Alcohol Treatment Records may only be Disclosed under (iii) of this particular Section.

4. **Abuse, Neglect, or Domestic Violence**. Covered Entity shall Disclose PHI, including, to the extent necessary and allowed by law, Special PHI about a minor Patient that Covered Entity reasonably believes to be a victim of abuse, neglect, or domestic violence, to a government authority (including a social service or protective services agency) that is authorized by law to receive such reports, which disclosure must be in line with Covered Entity's child abuse reporting policy. When Covered Entity makes such a Disclosure, it must promptly inform the Personal Representative unless that Covered Entity believes he or she is responsible

for the abuse or neglect and that it will not be in the minor's Patient's best interests to inform the Personal Representative.

5. **Health Oversight Activities**. Covered Entity shall Disclose PHI, as required by law, to health oversight agencies for oversight activities authorized by law (including audits, civil, criminal, or administrative investigations, inspections, licensure or disciplinary actions, and civil, criminal, and administrative proceedings). In addition, Disclosure is authorized for other activities necessary for the oversight of the health care system, a government benefits program (where the information is relevant to beneficiary eligibility), government regulatory programs (where the information is necessary for determining compliance with program standards), or to determine compliance with civil rights laws. Covered Entity may not Disclose PHI under this Section if the Patient is the subject of the investigation and the investigation is not directly related to the Patient's receipt of health care, claim for public health benefits, or qualification for or receipt of public health benefits when the Patient's health is integral to the claim for services.

6. **Judicial and Administrative Proceedings**. Covered Entity shall Disclose PHI in judicial and administrative proceedings in response to an order from a court or administrative tribunal, as long as the Disclosure is limited to the scope of the order, and as appropriate, must comply with 42 U.S.C. §290dd-3 and §290ee-3 (Drug and Alcohol Treatment Records) or other Special PHI Rules.

7. **To Avert a Serious Threat to Health or Safety**. Covered Entity will Disclose PHI, [subject to I.C. §34-30-16 et seq. (Duty to Warn) and I.C. §16-41-7 et seq. (Duty or Authority to Warn or Notify-Communicable Diseases)] if Covered Entity believes in good faith that the Disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Covered Entity's good faith will be presumed if it is based on actual knowledge or reliance on a "credible representation by a person with apparent knowledge or authority." Moreover, the Disclosure must be to a person reasonably able to prevent or lessen the threat (including to the target). If the Disclosure is because of a statement of a Patient admitting participation in a crime, Covered Entity may not Disclose the statement if it is obtained in the course of treatment to affect the propensity to commit the criminal conduct or through a request by the Patient to initiate or be referred for treatment. Moreover, such Disclosure must contain only the statement itself, plus the identifying information allowed by Subsection 3(i) of this particular Policy.

C. Pursuant to Certain Laws That "Permit" Disclosure by Covered Entity Without An Executed Authorization Form. As directed by the Privacy/Security Officer, and even without an executed Authorization Form, Covered Entity may Disclose a Patient's PHI in any of the following circumstances, provided that PHI that includes Mental Health Records, Drug and Alcohol Treatment Records, and Communicable Disease Records may only be Disclosed in accordance with I.C. §16-39-2 et seq., or I.C. §16-39-3 et seq. (Mental Health Records), 42 USC 290dd-3 or 42 USC 290ee-3 (Drug and Alcohol Treatment Records), and I.C. §16-41-2 et seq. (Communicable Disease Records):

1. **Communicable Diseases**: Covered Entity may Disclose PHI to a person who may have been exposed to a communicable disease or is at risk of contracting or spreading a disease if Covered Entity, or a public health authority, is authorized by law to notify the person, in accordance with I.C. §16-41-2-2 and §16-41-2-3.

2. **Subpoenas**: Covered Entity may Disclose PHI, excluding Special PHI unless allowed pursuant to the Special PHI rules for such records, under the following circumstances in response to a subpoena, discovery request, or other lawful process:

    a. **Written Notice to Patient**. The party seeking the information provides "Satisfactory Assurance" to Covered Entity that the party has made reasonable efforts to ensure that the Patient or Personal Representative, as applicable, has been given notice of the request. "Satisfactory Assurance" is a written statement and accompanying documentation demonstrating that: (i) the party seeking the information has made a good faith attempt to provide written notice to the Patient or Personal Representative; (ii) the notice included sufficient information about the litigation to permit the Patient or Personal Representative to raise an objection; and (iii) the time for the individual to raise objections has passed, and no objections were filed or the court resolved such objections against the Patient or Personal Representative. If Covered Entity does not receive such "Satisfactory Assurance," it may Disclose the PHI if Covered Entity itself makes reasonable efforts to provide notice to the Patient or seeks a qualified protective order.

    b. **Qualified Protective Order**. The party Seeking the information provides "Satisfactory Assurance" that the party has made reasonable efforts to secure a qualified protective order. This "Satisfactory Assurance" is a written statement and accompanying documentation demonstrating that: (i) the parties to the dispute have agreed to a qualified protective order and have presented it to the court or tribunal; or (ii) the party seeking the information has requested a qualified protective order from the court or tribunal. A "qualified protective order" is a court or tribunal order, or stipulation of the parties, that prohibits the parties from Using or Disclosing the PHI for any purpose other than the litigation or proceeding and that requires the return to Covered Entity or the destruction of the PHI at the end. If Covered Entity does not receive such "Satisfactory Assurance," it may Disclose the PHI only if Covered Entity makes reasonable efforts to provide notice to the Patient or seeks a qualified protective order.

    To confirm either of these "Satisfactory Assurances" with the requesting party in a timely manner, Covered Entity shall prepare a standard letter to send to any attorney or other requesting party who submits a subpoena, discovery request, or other lawful process to Covered Entity.

3. **Law Enforcement Purposes**: In the following circumstances, Covered Entity may Disclose PHI to law enforcement officials.

a. **Limited Information for Identification and Location Purposes**. When law enforcement officials request information to identify or locate a suspect, fugitive, material witness, or missing person Covered Entity may Disclose only limited information, including: (i) name; (ii) address; (iii) date and place of birth; (iv) social security number; (v) blood type; (vi) type of injury; (vii) date and time of treatment; (viii) date and time of death (if applicable); and (ix) a description of distinguishing physical characteristics (such as height, weight, gender, race, hair and eye color, and the presence or absence of facial hair, scars, and tattoos). Covered Entity may not Disclose PHI related to the Patient's DNA or DNA analysis, dental records, or typing, samples, or analysis of body fluids or tissue.

b. **Victims of a Crime**. When law enforcement officials request information about a suspected crime victim, Covered Entity may Disclose PHI if the Patient or Personal Representative consents to the Disclosure in writing.

c. **Decedents**. Covered Entity may Disclose PHI, excluding Mental Health Records, Drug and Alcohol Treatment Records, and Communicable Disease Records, including HIV/AIDS Records, about a Patient who has died for the purpose of alerting law enforcement of the death if Covered Entity suspects that the death resulted from criminal conduct.

d. **Crime on Premises**. When Covered Entity is providing emergency health care in response to a medical emergency, it may Disclose limited PHI, including, to the extent necessary and allowed by law, Special PHI in order to alert law enforcement to the commission and nature of a crime on its premises or against a person who works for Covered Entity or a threat to commit such a crime, the location of such crime or the victims, and the identity, description, and location of the perpetrator.

e. **Whistleblowers and Employee Crime Victims**. Workforce or Business Associate may Disclose PHI, either as a Whistleblower or as a victim of a criminal act, to law enforcement officers so long as the PHI Disclosed is about a suspected perpetrator of a criminal act and the PHI Disclosed is limited to: (i) name and address; (ii) date and place of birth; (iii) social security numbers; (iv) ABO blood type and rh factor; (v) type of injury; (vi) date and time of treatment; (vii) date and time of death, if applicable; and (viii) a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos.

4. **Coroners, Medical Examiners, and Funeral Directors**. Covered Entity may Disclose PHI, excluding Drug and Alcohol Treatment Records and Communicable Disease Records, to a coroner or medical examiner for the purposes of identifying a deceased person, determining a cause of death, or other duties authorized by law. In addition, Covered Entity may Disclose PHI to funeral directors as necessary to carry out their duties.

5. **Schools; Correctional Institutions and Other Law Enforcement Custodial Situations; Employers**. Should any request to disclose PHI to schools, correctional institutions, or employers be received by Covered Entity, that request shall be sent to the Security/Privacy Officer for review and response in order to comply with HIPAA and other applicable laws. The Privacy Officer shall not allow the disclosure of PHI to a school without an Authorization signed by the Personal Representative in the case of a minor Patient.

D. Pursuant To An Executed Authorization Form.

1. **Authorization Form**. Aside from any Uses and Disclosures that are expressly authorized by this Section, Covered Entity will not Use or Disclose any PHI for any other purpose or reason without first obtaining an executed Authorization Form from the minor Patient's Personal Representative, or otherwise confirming with the Privacy/Security Officer that the particular Use or Disclosure is otherwise permitted or required by applicable law or regulation. (**Attachment 13)**. In addition, Covered Entity may only disclose PHI on social media, including the image of a minor Patient, if it first obtains the Authorization for Disclosure on Social Media (**Attachment 12**).

2. **Records**. Covered Entity shall provide the minor Patient's Personal Representative with a copy of the executed Authorization Form.

3. **Expiration; Revocation**. The Patient or, if the Patient is a minor the Personal Representative, may revoke an executed Authorization Form in writing at any time prior to the expiration, but such revocation will not impact disclosures made prior to the revocation.

4. **May Not Condition Treatment**. Covered Entity shall not in any way condition the provision of Treatment to the Patient on the execution of an Authorization Form by the Patient, except where the provision of Health Care is solely for the purpose of creating PHI for Disclosure to a third party.

E. Validation Procedure for Disclosures of PHI and ePHI Contrary to This Policy. Any Disclosure of PHI or ePHI contrary to this Policy requires the prior approval of the Privacy/Security Officer.

F. Prohibition on Sale of PHI. Any Disclosure of PHI by Covered Entity to a third party in exchange for direct or indirect payment that otherwise qualifies as a Sale of PHI is strictly prohibited by HIPAA and these Policies. Subject to this prohibition, the following limited exceptions apply where the purpose of the exchange is for: Public health activities conducted in accordance with 45 C.F.R. § 164.512(b).

1. Research activities conducted in accordance with 45 C.F.R. § 164.501 and 164.512, and the price charged reflects the cost of preparation and transmittal of data for such purposes.

2. Conducting Health Care Operations as defined by 45 C.F.R. § 164.501.

3. Is for the sale, transfer, merger, or consolidation of all or part of Covered Entity and for related due diligence (if applicable).

4. Payment by Covered Entity to a Business Associate for activities that the Business Associate undertakes on behalf of Covered Entity and at the specific request of Covered Entity pursuant to a Business Associate Agreement or on behalf of a Business Associate in the case of a sub-contractor.

5. Providing a Patient with a copy of his/her PHI in accordance with 45 C.F.R. § 164.524.

6. Any other purpose permitted by and in accordance with the HIPAA Privacy Rule, 45 C.F.R. §164.502, where the only remuneration (the thing of value) received by Covered Entity or Business Associate, acting on Covered Entity's behalf, is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

7. Covered Entity's Privacy/Security Officer must approve any Disclosure of PHI in exchange for Remuneration to confirm that it does not otherwise qualify as Sale of PHI and that at least one of the exceptions described above applies.

ARTICLE IV
HOW COVERED ENTITY WILL MANAGE PATIENTS' INDIVIDUAL RIGHTS REGARDING THEIR PROTECTED HEALTH INFORMATION

A. **Right to Notice of Privacy Practices**. Each Patient and Personal Representative has the right to receive a current copy of Covered Entity's Notice of Privacy Practices (Attachment 12). Covered Entity shall make and document a good faith effort to provide this Notice to all current Patients or, in the case of minors, Personal Representatives. The Patient, or in the case of minor's, shall receive a notice of any amendment to this Notice. Covered Entity shall make a good faith effort to obtain the Patient's written acknowledgment that the Patient has received all such Notices and amendments by having the Patient sign a copy of the Patient Acknowledgement Form (Attachment 13). If Covered Entity is unable to obtain the Patient's signature or a copy of the Acknowledgement Form, despite its good faith efforts, Covered Entity shall document same on the Patient Acknowledgment Form and continue to make reasonable attempts thereafter. The Patient shall receive a copy of the executed form.

B. **Right to Request Certain Restrictions on PHI Uses and Disclosures**.

1. Each Patient or their Personal Representative, in the case of minors, has the right to request that Covered Entity:

   a. not Use or Disclose certain PHI for the purposes of providing Treatment, obtaining certain Payments, or performing Health Care Operations;

   b. not Use or Disclose certain PHI in order to perform Payment functions if the PHI pertains to a Health Care Service for which the Patient agrees to pay Covered Entity, out of pocket, in full, at the time of service;

c. not Disclose certain PHI to certain of the Patient's family members or friends who may be involved in the Patient's care or for other notification purposes described in the Privacy Notice; or

d. communicate with the Patient regarding upcoming appointments, treatment alternatives, and the like by contacting the Patient at a specific telephone number or address designated by the Patient.

2. The Personal Representative must submit a completed Patient Request to Restrict PHI Uses and Disclosures Form to the Privacy/Security Officer (**Attachment 9**).

3. Covered Entity has an obligation to accommodate all reasonable Patient requests that are not too difficult for Covered Entity to administer. The Privacy/Security Officer shall either approve or deny the Patient's request and complete the Form in a timely manner. If approved, the Privacy/Security Officer shall inform Workforce and related instructions shall be noted on Patient's contact sheet.

4. Whether the Patient's request is approved or disapproved, the Patient shall receive a copy of the completed Form, and the original shall be noted on and placed behind the Privacy Flow Sheet under the Privacy Tab in the appropriate Patient Record.

5. The Patient may revoke an approved request at any time as long as such revocation is in writing, received by the Privacy/Security Officer, and noted on the Patient's contact sheet. Any amendment of an approved request requires the Patient to submit a new Patient Request Form to the Privacy/Security Officer.

C. <u>Right to Request Access to PHI</u>.

1. Each Personal Representative has the right to request the opportunity to inspect and/or receive a copy of part or all of the PHI contained in the Patient's Patient Record maintained by Covered Entity; provided, however, that Covered Entity may deny Disclosure under certain circumstances, as follows:

a. A licensed professional has determined that Access may endanger life or safety.

b. There is reference to another person and Access may cause harm.

c. The request is made by Personal Representative who may cause harm.

d. The PHI requested is Psychotherapy Notes.

e. The PHI is compiled for a legal proceeding.

f. The PHI is subject to CLIA.

g. The PHI is the subject of research to which denial of Access has been agreed.

h. The PHI is obtained from a third party in confidence and is not subject to further review.

2. Covered Entity may accept a Personal Representative's request to Access PHI, either in writing or verbally; however, Covered Entity shall encourage Personal Representatives to make all such requests, if at all possible, by submitting a completed Patient Request to Access Form to the Privacy/Security Officer. Any verbal requests must be documented by Covered Entity in the Patient's record. (**Attachment 16)**

3. Covered Entity shall approve or deny the request, complete the Form in a timely manner, and produce the PHI to Patient as soon as practicably possible and without any unreasonable delay, but no later than thirty (30) days following the request. Covered Entity may obtain a thirty (30) day extension but only after notifying Patient of the reasons for the extension, in writing. If Patient access is denied, Covered Entity must provide the Patient with a timely, written explanation in plain language of:

   a. the basis for the denial;

   b. the Patient's review rights (if any) under HIPAA and applicable state law;

   c. how to file a Complaint with Covered Entity and/or HHS' Office for Civil Rights; and

   d. the source of the PHI not maintained by Covered Entity, if known.

   Covered Entity must also give the Patient Access to any part of the PHI not covered by the Privacy/Security Officer's denial.

4. **Review Rights**.

   a. A decision by the Privacy/Security Officer to deny the Access, because (i) a licensed professional has determined that Access may endanger life or safety, (ii) there is reference to another person and Access may cause harm, or (iii) the request was made by Personal Representative who may cause harm, is subject to further review by the President of Covered Entity or their designee to determine whether the original Privacy/Security Officer decision shall be upheld, reversed, or otherwise modified and to notify the Patient and the Privacy/Security Officer in writing.

   b. A decision by the Privacy/Security Officer to deny the Patient's Access, because the PHI is (i) psychotherapy notes, (ii) compiled for legal proceeding, (iii) subject to CLIA, or (iv) obtained from a third party in confidence and is not subject to further review.

5. If the Patient is permitted a copy of part or all of the PHI, then Covered Entity personnel shall be informed and given any related instructions, and the Patient shall

be sent the PHI in the manner requested by the Patient, subject to the Covered Entity ensuring that such manner is feasible and secure.

D. <u>Right to Request Amendment of PHI</u>.

1. Each Personal Representative has the right to request, in writing, that PHI maintained by Covered Entity with regard to the Patient be amended or corrected.

2. The Personal Representative must submit a completed Patient Request to Amend PHI Form to the Privacy/Security Officer (**Attachment 17**).

3. **<u>Reasonable and Timely Response</u>**.

   a. The Privacy/Security Officer may deny the requested amendment if: (i) the PHI was not created by Covered Entity, unless the Personal Representative provides evidence that the originator is no longer available to act on the request; (ii) the amendment concerns PHI that is not a part of the Patient Record; (iii) the PHI is not available for access; or (iv) the PHI is deemed to be accurate and complete.

   b. The Privacy/Security Officer shall approve or deny the request, complete the Form accordingly, and notify the Personal Representative whether the request has been approved or denied within thirty (30) days of the request.

   c. If the requested amendment is approved, the Privacy/Security Officer shall append or link the amendment to the Patient Record and notify the relevant person(s) with whom the amendment needs to be shared.

   d. If the requested amendment is denied, Covered Entity must provide the Patient with a timely, written explanation in plain language of: (i) the basis for the denial; (ii) the Personal Representative's right to submit a written statement of disagreement; (iii) the Personal Representative's right to request that Covered Entity include documentation of the request, Covered Entity's denial, the Personal Representative's disagreement, and any rebuttal by Covered Entity with any subsequent disclosure of the subject PHI by Covered Entity; and (iv) how to file a Complaint with Covered Entity and/or the Office for Civil Rights.

   e. If the Personal Representative does not submit a written statement of disagreement to Covered Entity, Covered Entity must include only documentation of the request and Covered Entity's denial in subsequent disclosure of the subject PHI by Covered Entity, but only if the Personal Representative has requested such action in writing.

4. Whether the Patient's request is approved or disapproved, the Personal Representative shall receive a copy of the Form, and the original shall be noted on, and placed behind, the Privacy Flow Sheet under the Privacy Tab in the appropriate Patient Record.

E. **<u>Right to an Accounting of PHI Disclosures</u>**.

1. Each Patient or Personal Representative, as applicable, has the right to request an accounting of any PHI Disclosed by or on behalf of Covered Entity to a third party during the six (6) years preceding the date of the written request, except for Disclosures:

    a. to carry out Treatment, Payment, and Health Care Operations;

    b. to the Patient, to other persons involved in the Patient's care, or for other notification purposes in accordance with these Policies;

    c. pursuant to a written authorization signed by the Patient in accordance with these Policies;

    d. for national security or intelligence purposes or to Correctional Institutions or law enforcement officials, as appropriate; or

    e. as part of a Limited Data Set for purposes of and in accordance with 42 CFR § 164.514(e);

    any of which occurred prior to April 14, 2003.

2. The Patient or Personal Representative must submit a completed Patient Request for Accounting of PHI Disclosures Form to the Privacy/Security Officer. (**Attachment 18**)

3. **<u>Reasonable and Timely Response</u>**.

    a. The Privacy/Security Officer shall act upon the request within thirty (30) days of receipt of the written request by providing the Patient or Personal Representative with a written report. If Covered Entity is unable to provide the accounting within the time frame, the Privacy/Security Officer may extend the time by no more than thirty (30) days, provided that the Patient receives prior written notice of the reason(s) for the delay.

    b. The first accounting provided in any 12-month period must be provided without charge. A reasonable, cost-based fee may be charged for subsequent accountings within the same 12-month period if the Patient or Personal Representative receives prior written notice.

    c. The Privacy/Security Officer shall temporarily suspend a Patient's right to an accounting of disclosures to health oversight agencies or law enforcement officials if the agency or official provides a written statement to Covered Entity that the accounting will impede their activities.

4. Whether the accounting is performed or not, the Patient or Personal Representative shall receive a copy of the Form, and the original Form shall be noted on, and placed

behind, the Privacy Flow Sheet in the appropriate Patient Record.

F. Right to Notification of Breach Involving Unsecured PHI or Other Unauthorized Access to Personal Information.

1. Each Patient has the right to receive from Covered Entity a written notice of any Breach involving Unsecured PHI or other Unauthorized Access of Personal Information pertaining to the Patient so that, among other things, the Patient may institute the procedures necessary to decrease the risk of possible misuse of his/her PHI and/or other Personal Information, which may result in Identity Deception or Theft or other fraud.

2. Any written notice to a Patient regarding a Breach involving Unsecured PHI or other Unauthorized Access of Personal Information shall be completed without unreasonable delay.

3. A copy of the written notice provided to the Patient shall be placed in the Privacy Flow Sheet of the appropriate Patient Record.

G. Right to Contact Privacy/Security Officer and File a Complaint.

1. Regarding "Complaints and Incidents," each Patient has the right to contact the Privacy/Security Officer at any time with questions, comments, or complaints about privacy practices or if the Patient believes Covered Entity violated his/her privacy rights.

2. Each Patient has the right to contact HHS' Office for Civil Rights regarding these privacy matters, particularly if the Patient does not believe that Covered Entity has been responsive to his/her concerns.

ARTICLE V
HOW COVERED ENTITY WILL MANAGE CONTRACTUAL RELATIONSHIPS WITH BUSINESS ASSOCIATE RELATIONSHIPS

A. Roster; Agreement or Addendum. The Privacy/Security Officer shall maintain a current and complete roster of the Business Associates of Covered Entity. Any person or entity that qualifies as a Business Associate of Covered Entity must enter into a Business Associate Agreement or Addendum.

B. Vendors and Other "Business Visitors". Any person or entity that provides services for or on behalf of Covered Entity that does not require, but which may result in certain Incidental Access to PHI, shall enter into a Vendor Agreement as approved by Covered Entity. Should the Vendor qualify as a Business Associate of Covered Entity, the Vendor shall also enter into a Business Associate Agreement with such vendor. Any person or entity that provides services on behalf of an individual Patient shall enter into a Service Provider Access Agreement.

ARTICLE VI
HOW COVERED ENTITY WILL SAFEGUARD PROTECTED HEALTH

INFORMATION FROM UNAUTHORIZED ACCESS

A. Access Controls.

1. **Premises and Workstations**. Covered Entity shall provide physical Access to Covered Entity premises only to authorized Workforce and to minor Patients, their Personal Representatives, and other guests of the minor Patient's family. Covered Entity may also allow for invitees and guests to have access to Covered Entity's premises so long as they do not have access to PHI and have signed a Visitor Confidentiality Agreement unless such access has been granted by an Authorization or otherwise allowed pursuant to these Policies. Covered Entity shall permit physical/electronic access to Workstations only to authorized Workforce. Workforce must ensure that all PHI in hardcopy or electronic form is removed from their workspace and secured in a drawer when the desk is unoccupied and at the end of the work day.

2. **Keys and Passwords**. Covered Entity shall issue keys and other access tokens (e.g., card, combination, etc.) to Covered Entity premises and passwords and other access privileges to PHI and ePHI only to those Workforce authorized by the Privacy/Security Officer. All such Workforce are required: (a) not to use a key or password, other than those assigned, to Access any PHI of Covered Entity for unauthorized purposes; (b) to safeguard their assigned keys and passwords from unauthorized Use by a third party; (c) to lock all premises, or log off from any computer or other Electronic Media, as soon as any authorized Access has been completed; and (d) to select, secure, and update, as necessary, "strong" passwords that comply with Covered Entity's password policy.

3. **Unauthorized Software Downloads**. No software shall be loaded or downloaded from the Internet onto Covered Entity computers without the prior authorization by the Privacy/Security Officer.

4. **Malicious Software**. Covered Entity shall install and regularly update the necessary anti-virus software on all Electronic Media that is used to Access ePHI by Covered Entity and its Workforce and Business Associates.

5. **Response to Incidents**. Covered Entity shall comply with its contingency plan in its response to any emergency, disaster, or other comparable Incident that threatens the Confidentiality, Integrity, or Availability of ePHI created or maintained by Covered Entity at all times. All such actions to repair and/or restore ePHI during or following an Incident shall be conducted under the direct and personal supervision of the Privacy/Security Officer (or designee) at all times.

6. **Internet**. Workforce shall limit incidental non-official access to the internet and shall not attempt to view web content that violates Covered Entity's anti-harassment or discrimination policies.

B. Workforce Controls.

1. **Screening; Training**. Covered Entity shall screen and train its Workforce in accordance with those procedures set forth in the applicable policies of Covered Entity in order to select those qualified Workforce who may be authorized to Access, Use, Modify, Disclose, or Destroy certain PHI of Covered Entity, under certain limited circumstances, as specified in the particular User's position description or applicable Minimum Necessary Standards of Covered Entity.

2. **Monitoring and Audit; Supervision**. Covered Entity shall conduct the necessary monitoring and audit procedures to confirm and correct, if necessary, Workforce compliance and the incidence of any Security Incidents in violation of these Policies.

3. **Corrective Action**. The Privacy/Security Officer shall oversee corrective action measures to address noncompliance findings, and where appropriate, shall follow sanctions for specific violations in accordance with these policies.

4. **Reporting**. Workforce shall report activities by any other individual or entity that they suspect may compromise the confidentiality of PHI to the Privacy/Security Officer. Reports are made in good faith and will be held in confidence to the extent permitted by law. Retaliation for a good faith report of a violation of law or policy is prohibited.

5. **Termination**. Upon termination, or any other material change in the status of a Workforce or Business Associate, the Privacy/Security Officer, in conjunction with the President of Covered Entity (or designee) or the Human Resources Director, will terminate, retrieve, or otherwise amend the person's Access to PHI of Covered Entity and document same on the appropriate PHI Access Checklist. The particular Workforce or Business Associate shall also agree, in writing, to maintain the continuing confidentiality of all PHI of Covered Entity at all times following termination.

C. Electronic Media Controls.

1. **Electronic Media**. The Privacy/Security Officer shall account for all new or used Electronic Media (e.g., laptops, tablets, iPADs, smart phones, etc.) acquired by Covered Entity that are to be used to Access PHI on or off Covered Entity premises. All such Electronic Media shall be encrypted in accordance with standards approved by the Privacy/Security Officer and HHS' Office for Civil Rights. Additionally, each Workforce shall complete a written Workforce Confidentiality Agreement (**Attachment 3**), which Agreement may be amended by Covered Entity.

2. **Back Up**. The Privacy/Security Officer (or designee) will institute a regular procedure to "back up" all PHI created and maintained in an electronic format by Covered Entity in the form of a retrievable, exact copy. The "back up" copies shall be encrypted and stored in a secure off-site location or secure cloud.

3. **Off Premises Use**. No PHI, regardless of its form or medium, or Covered Entity-

owned Electronic Media containing e-PHI should be taken off Covered Entity premises unless otherwise approved, in advance, by the Privacy/Security Officer and only for authorized purposes (e.g., to transport original Patient records to different office location). Covered Entity shall "check out" all PHI taken off premises and "check in" the PHI upon return (no later than 24 hours later) according to established office procedures approved by the Privacy/Security Officer. While any such PHI or Electronic Media is off Covered Entity premises, the Workforce shall Use, maintain, and store the PHI and Electronic Media in a secure manner and location that is under the User's personal control and custody (e.g., locked trunk of car, locked vehicle lacking trunk and out of view; locked residence; locked file cabinet, or other secure storage).

4. **Immediate Report of Any Lost or Stolen Devices**. All Workforce shall immediately report to the Privacy/Security Officer any Covered Entity-owned computer or mobile device that is lost or stolen. Additionally, all Authorized Workforce under (3) above shall immediately report to the Privacy/Security Officer any personal computer or mobile devices that are lost or stolen and which had been used to conduct Covered Entity business or to otherwise, create, transmit or store any Patient's PHI.

D. Communication Controls.

1. **Telephone Calls**. Covered Entity may communicate with the minor Patient's Personal Representative regarding upcoming appointments, treatment alternatives. If voicemail is received, the Workforce shall not leave any detailed PHI on the voicemail. No Workforce may Disclose any PHI or other verbal information regarding a Patient to any third party, by telephone or otherwise, unless and until the Workforce is so authorized and has (1) confirmed the name and address of the caller and the purpose of the call, (2) whether the caller qualifies as a "next of kin" identified by the Patient and documented in the Patient Record, and if so, (3) whether the caller knows the particular Patient identifiers (e.g., birth date, social security number, account number, etc.) that are required before Disclosing any information about the Patient's PHI to the caller. If a caller is not confirmed as an authorized recipient of PHI for that Patient, the Workforce shall coordinate the request with the Patient's Legal Representative and the requestor in a manner authorized by this Policy.

2. **Mail**. Covered Entity may communicate with the Personal Representative regarding upcoming appointments, treatment alternatives, and the like by contacting the Personal Representative at an address provided by the Personal Representative. Any communications to a Personal Representative by mail shall be enclosed in a sealed envelope.

E. Electronic Communication Controls.

1. **Covered Entity Website**. The Covered Entity website should contain a link to the Notice of Privacy Practices.

2. **E-Mail**. No Workforce may prepare, save, or send any e-mail communication containing PHI to any person or entity, beyond Covered Entity's fire-wall-protected Intranet, unless Covered Entity has approved and installed acceptable encryption software to secure the e-mails. Workforce will not use personal email accounts for transmitting or receiving Covered Entity information or conducting Covered Entity business except for multi-factor authentication purposes. Workforce will not send e-mail that violates Covered Entity policy.

3. **Text Messages**. No Workforce may prepare, save, or send any text message communications containing PHI to any person or entity unless required for Patient Treatment, care or coordination and no other reasonable alternative is available, and in those instances text message should only be utilized when needed to resolve immediate issues Text messages should not contain any identifiable PHI and if any text message received by Workforce do contain PHI they should be immediately and permanently deleted.

4. **Personal Electronic Media**. Any Workforce who intends to use their own Electronic Media to Access PHI for authorized purposes shall be required to institute certain safeguards which are set forth in the Workforce Confidentiality Agreement that shall be signed by Workforce to confirm their compliance with all applicable requirements as a condition of employment or other affiliation with Covered Entity.

5. **Facsimile**. All facsimile machines of Covered Entity shall be in a secure location or otherwise in a location not accessible by the public. Workforce shall take reasonable steps to assure that facsimile transmissions are sent to the appropriate destination. A coversheet must be used for all facsimiles that contains the recipient's name, a notation that protected health information is being sent and that the facsimile is confidential, and information on who to contact if the facsimile is not sent to the intended recipient. If Workforce becomes aware that a facsimile has been misdirected, the unintended receiver must be contacted immediately by Workforce, acting in conjunction with the Privacy/Security Officer, in order to mitigate the risk of compromise to the PHI contained in the facsimile documents.

6. **Storage Controls**. Covered Entity shall store all PHI in a secure location, either on the premises of Covered Entity, or at an off-site location as appropriate, pursuant to the terms and conditions set forth in a Business Associate Agreement or Addendum.

7. **Removal, Destruction, and Disposal Controls**. Any original copies of a Patient Record, or alternatively any PHI or ePHI, of Covered Entity that Covered Entity or its Business Associate intends to destroy must be rendered absolutely unusable, unreadable, and undecipherable, such as by shredding or removal and destruction of hard drives from laptops.

8. **Social Media**. No Workforce member shall ever post or otherwise disclose any PHI which concerns any Patient on the Internet, on Facebook or other social media

without first obtaining an Authorization (**Attachment 10**) and complying with Covered Entity's Social Media Policy.

ARTICLE VII
GLOSSARY OF TERMS

Adult means a person eighteen (18) years of age or older. If, under Indiana law, a person has authority to act on behalf of a Patient who is an adult or an emancipated Minor in making decisions related to health care, Covered Entity will treat such person as a Personal Representative with respect to PHI relevant to such Personal Representative.

Authorization or Authorization Form means the mechanism for obtaining a Patient's written authorization of Covered Entity's Use or Disclosure of PHI for functions or activities that are not related to providing Treatment, obtaining Payment, or performing Health Care Operations, or that are not otherwise permitted or required by applicable law or regulation.

Breach means any acquisition, access, or Use or Disclosure of PHI which compromises the Security or Privacy of the PHI and poses a significant risk of financial, reputational, or other harm to an individual. An acquisition, access, or Use or Disclosure of PHI in a manner not permitted is presumed to be a breach unless Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of: (i) the nature and extent of the PHI involved (including types of identities and likelihood of re-identification); (ii) the unauthorized person who used the PHI or to whom the Disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.

However, the term "Breach" does not include (a) any unintentional acquisition, access, or Use of PHI by Workforce or other individual acting under the authority of Covered Entity or a Business Associate if such acquisition, access, or Use of PHI is made in good faith and within the course and scope of employment or other professional relationship, as appropriate, and the PHI is not further acquired, accessed, Used, or Disclosed by any person; (b) any inadvertent Disclosure by Workforce or other individual acting under the authority of Covered Entity or a Business Associate if to another similarly situated Workforce or individual, and the PHI is not further acquired, accessed, Used, or Disclosed without Authorization by any person; or (c) any Disclosure of PHI where Covered Entity or a Business Associate has a good faith belief that an unauthorized person to whom the Disclosure is made will not reasonably be able to retain such information.

Business Associate means a person or entity who creates, receives, maintains, or transmits PHI for a function or activity on behalf of, or provides a specified service to or for, the Covered Entity. A Business Associate includes an entity that provides services related to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, repricing, legal actuarial, accounting, consulting, data aggregation, if those services involves the creation, receipt, maintenance, or transmission of PHI.

The term "Business Associate" does not include: (a) health care providers, with respect to Disclosures by Covered Entity to the health care provider concerning Treatment of the Patient; (b)

a plan sponsor, with respect to disclosures by a group health plan (or health insurance issuer or HMO) to the plan sponsor as long all other Disclosure requirements are met; and, (c) a government agency, for determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent authorized by law.

Communicable Disease Records means recorded or unrecorded medical or epidemiological information involving a communicable disease or other disease that is a danger to health, including HIV/AIDS Records.

Complaint means any communication by any person to Covered Entity that identifies any specific questions, concerns, or actual complaints regarding Covered Entity's compliance with these Policies.

Deceased Person means a person who is no longer alive. If, under Indiana law, an executor, administrator, or other person has authority to act on behalf of a Deceased Person, or on behalf of a person's estate, Covered Entity will treat such person as Personal Representative with respect to PHI relevant to such Personal Representative.

Deceased Patient Record means PHI of the Deceased Person that relates to the family member, other relative, close personal friend, or other person's involvement in the Deceased Person's care or Payment for Health Care prior to the Deceased Person's death.

De-Identified means a Health Information that is not individually identifiable because all identifiers of the individual and his/her relatives, employers, and household members have been deleted in accordance with 45 CFR 164.514(b), and the Covered Entity does not have actual knowledge that the information can be used alone or in combination with other information to identify an individual who is a subject of the information.

Direct Treatment Relationship means a treatment relationship between a health care provider and a Patient in which: (i) the health care provider delivers health care to an Individual in accordance with Covered Entity's own plan or care or orders; and (ii) the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to the Patient.

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

Drug and Alcohol Treatment Records means any information, whether or not recorded, which will identify a Patient as an alcohol or drug abuser either directly, by reference to other publicly available information, or through verification of such an identification by another person and information which can be used for the purpose of treating alcohol or drug abuse, making a diagnosis for the treatment, or making a referral for the treatment.

Electronic Media means electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. Electronic media also includes transmission media used to exchange

information already in electronic storage media, such as: the internet; extranet or intranet; leased lines; dial-up lines; private networks; and physical movement of removable/transportable electronic storage media. Certain transmission, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Encryption or Encrypted means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential or secondary authentication.

Health Care means care, services, or supplies related to the health of a Patient, including, but not limited to the following: (i) preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling service, assessment, or procedure with respect to the physical or mental condition or functional status of a Patient or that affects the structure or function of the body; and (ii) the Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Operations means certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501.

Health Information means any information, whether oral or recorded in any form or medium, that: (i) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house; and (ii) relates to the past, present, or future physical or mental health or condition of a Patient, the provision of health care to a Patient, or past, present, or future payment for the provision of health care to a Patient.

Health Oversight Agency 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 authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Incident means a Complaint, any evidence of a successful Security Incident, Breach, or other Unauthorized Access to PHI.

Incidental Use and Disclosure means those Uses and Disclosures that are incidental to an otherwise permitted Use or Disclosure.

Indirect Treatment Relationship means a relationship between a Patient and a health care provider in which: (i) the health care provider delivers health care to a Patient based on the orders of another health care provider; and (ii) the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to a Patient.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from a Patient, and: (i) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (ii) relates to the past, present, or future physical or mental health or condition of a Patient or genetic testing conducted on a Patient, the provision of health care to a Patient, or the past, present, or future payment for the provision of health care to a Patient; and (iii) that identifies the Patient or with respect to which there is a reasonable basis to believe the information can be used to identify the Patient.

Limited Data Set means Protected Health Information that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual: (i) name; (ii) postal address information, other than town or city, state, and zip code; (iii) telephone numbers; (iv) fax numbers; (v) electronic mail addresses; (vi) social security numbers; (vii) health plan beneficiary numbers; (viii) medical record numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) Web Universal resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.

Mental Health Records means recorded or unrecorded information concerning the diagnosis, treatment, or prognosis of an Individual receiving mental health services or developmental disability training. The term does not include alcohol and drug abuse records.

Patient means the person who is the subject of the Protected Health Information, and in certain cases, the term also means the Individual's Personal Representative.

Patient Record means those records maintained by or on behalf of Covered Entity that are: (i) the medical records and billing records about particular Patients of Covered Entity that are maintained by or for Covered Entity; and (ii) used, in whole or in part, by or for Covered Entity to make decisions about its Patients. For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for Covered Entity.

Payment means: (i) the activities undertaken by Covered Entity to obtain or provide reimbursement for the provision of health care; and (ii) the activities in paragraph (i) of this definition relate to the Individual to whom health care is provided and include, but are not limited to: (1) determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (2) risk adjusting amounts due based on enrollee health status and demographic characteristics; (3) 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; (4) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (5) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (6) disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement (Name and

address; Date of Birth; Social Security number; Payment history; Account number; and Name and address of the health care provider and/or health plan.)

Personal Information means that nonpublic information which is further described in the Summary of Indiana Laws Governing Personal Information, a copy of which is available under Section I.B. of this Policy. Personal Information does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records. For purposes of this Policy, the capitalized term Personal Information qualifies as PHI as that capitalized term is defined here.

Personal Representative means a person who has legal authority to act on behalf of a Patient with respect to health care decisions and to obtain copies of a Patient's PHI, and includes the parents of a minor Patient. Covered Entity may not elect to treat a person as Personal Representative of a Patient if (i) Covered Entity has a reasonable belief that the Individual has been, or may be, subjected to domestic violence, abuse, or neglect by such person, or treating such person as the Personal Representative may endanger the Individual, and (ii) Covered Entity, 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.

Privacy Flow Sheet means the record placed in the Patient Record that notes all necessary forms, communications, and other information received from the Individual. All forms executed by the Individual shall be placed behind the Privacy Flow Sheet under the Privacy Tab of the appropriate Patient Record.

Protected Health Information (PHI) means Individually Identifiable Health Information that is: (i) transmitted by Electronic Media; (ii) maintained in any medium described in the definition of Electronic Media at 45 C.F.R. §162.103 of this subchapter; or (iii) transmitted or maintained in any other form or medium. PHI excludes individually identifiable health information in: (i) education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) employment records held by a covered entity in its role as employer; and (iv) in regard to a person who has been deceased for more than 50 years.

Provider means a provider of services (as defined in §1861(u) of the Social Security Act), a provider of medical or health care services (as defined in §1861(s) of the Social Security Act), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business, also referred to herein as the "Covered Entity."

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 Patient'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.

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 whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Redacted means the alteration or truncation of data so that not more than the last four (4) digits of certain Personal Information, specifically the driver's license number, a state identification number, or an account number, or alternatively, no more than the last five (5) digits of a Social Security Number, are accessible as part of the Personal Information.

Re-Identified means information that has been De-Identified in this Policy and subsequently altered so that the de-identification process is no longer affected.

Sale of PHI means a Disclosure of PHI by Covered Entity or a Business Associate, where Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. However, Sale of PHI does not include a Disclosure of PHI : (i) for public health purposes; (ii) for Research purposes where the only remuneration received by Covered Entity or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purpose; (iii) for Treatment and Payment purposes; (iv) for the sale, transfer, merger, or consolidation of all or part of Covered Entity and for related due diligence; (v) to or by a Business Associate for activities that the Business Associate undertakes on behalf of Covered Entity (or on behalf of a Business Associate in the case of a Subcontractor), and the only Remuneration is by Covered Entity or Business Associate for the performance of such activities; (vi) to a Patient, when the purpose of the exchange is to provide the Patient with a copy of his or her PHI pursuant to the Patient's right to access and right to accounting of disclosures; (vii) when required by law; and (viii) for any other purpose permitted, where the only remuneration received by Covered Entity or Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

Security Incident means any attempted or successful effort to accomplish unauthorized access (e.g., Access, Use, Disclosure, Modification, or Destruction) of ePHI or to otherwise interfere with ePHI system operations in violation of these Policies.

Special PHI means Drug and Alcohol Treatment Records, Mental Health Records, and Communicable Disease Records, all of which are specially protected under applicable laws and regulations.

Subcontractor means a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the Workforce of such Business Associate.

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (i) health care claims or equivalent encounter information; (ii) health care payment and remittance advice; (iii) coordination of benefits; (iv) health care claim status; (v) enrollment and disenrollment in a health plan; (vi) eligibility for a health plan; (vii) health plan premium

payments; (viii) referral certification and authorization; (ix) first report of injury; and (x) health claims attachments.

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 an Individual for health care from one health care provider to another. The term "Treatment" also includes a communication made to a Patient: (i) to describe a health-related product or service that is provided by Covered Entity, including communications about Covered Entity's participation in a particular health care provider, health plan, or provider network; (ii) for Treatment of the Patient; or (iii) for case management or care coordination for the Patient, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the Patient.

Unencrypted means not encrypted.

Unredacted means not redacted.

Unsecured PHI means that PHI which is not secured through the use of a methodology, or alternatively, or that ePHI which is not secured through the use of a technology, any of which will otherwise make the PHI or ePHI unusable, unreadable, or indecipherable to unauthorized persons.

Validation is the act of ensuring that a person who requests Disclosure is an appropriate person to receive such information.

Workforce means any employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Covered Entity, is under the direct control of Covered Entity, whether or not they are compensated by Covered Entity.

Workstation means any Electronic Media maintained by Covered Entity that is used to Access PHI electronically, including but not limited to computer desktops, laptops, tablets, fax machines, or otherwise.

Attachment 1
POTENTIAL PRIVACY LAWS

Covered Entity may consult the following federal and state privacy laws listed on Attachment 1 while providing services to its patients as may be applicable:

The Health Insurance Portability and Accountability Act of 1996 and the related Privacy and Security Regulations ("HIPAA"), including 45 C.F.R. parts 160, 162 and 164.

- Indiana laws governing Social Security Numbers or credit card and banking information.
- Indiana laws governing health records and mental health records. See IC 16-39 et seq.
- Indiana laws governing communicable disease records. See IC 16-41-8-1.
- Indiana laws governing genetic records. See IC 16-39-5-2 and 27-8-26-2.
- Indiana laws governing security breaches. See IC 4-11-11-1
- Indiana laws governing health records. See IC 16-39 et seq

Attachment 2
HIPAA PRIVACY/SECURITY TRAINING HANDOUT

What is HIPAA?

HIPAA, the Health Insurance Portability and Accountability Act of 1996, is a law that safeguards the privacy and security of identifiable health information about our Patients. It includes what we must do to maintain this privacy and security, and the punishments for anyone caught violating this important law.

The Office for Civil Rights of the U.S. Department of Health and Human Services ("HHS") is the government agency authorized to enforce HIPAA's privacy and security regulations. The privacy regulations took effect in 2003, and the security regulations took effect in 2005. The state attorneys' general offices can also investigate these matters.

What is Confidential?

All information about our Patients is private or "confidential", whether written on paper, saved on a computer, or spoken aloud. This includes their name, address, age, Social Security number, and any other personal information. It also includes their photograph or any videos the Patient while receiving therapy. It also includes information about the therapy the Patient is receiving, caregiver information, any information about past health conditions, future health plans, and why the Patient requires our services.

Spoken communication includes discussing therapy treatment with a Patient or their Personal Representative, whispering in the hallway about Patients, and talking on the telephone about or to Patients or their Personal Representatives. Written communication includes the hard copy of the medical record, medication records, faxes, letters, forms, or any paper exchange of information. Electronic communication includes computerized medical records, electronic billing and e-mail. If you reveal any of this information to someone who does not "need to know" it, you have made an unauthorized disclosure, and you have broken the law.

What are the Consequences of Breaking the Law?

The consequences will vary, based on the severity of the violation, whether the violation was intentional or unintentional, or whether the violation indicated a pattern or Covered Entity of improper Use or Disclosure of identifiable health information.

Depending on the violation, Covered Entity may be fined by the government for non-compliance with HIPAA regulations. Covered Entity and their employees can receive civil penalties up to $50,000 for each violation subject to a $1.5 Million cap. Providers and their employees can also receive criminal penalties up to a $250,000 fine and/or 10 years in prison for using information for commercial or personal gain or malicious harm.

Why are Privacy and Security Important?

Our Patients and their Personal Representatives need to trust us before they will feel comfortable enough to share their health and other personal information with us. In order for us to provide quality care, we must have this information. They must know that whatever they tell us will be kept confidential and we will limit access to that information to only those individuals who need the information for treatment, payment, and Health Care Operations.

What is the "Need to Know" Rule?

This rule is really common sense. If you need to see Patient information to perform your job, you are allowed to do so. But, you may not need to see all of the information about every Patient. You should only have access to what you need to in order to perform your job.

There may be occasions when you will have access to confidential information that you don't need for your work. For example, you may see information on whiteboards or sign-in sheets. You may also see Patients and their Personal Representatives walking around or facility or receiving therapy. You must keep this information confidential.

There is no doubt that you will overhear private health information as you do your day-to-day work. You must keep this information confidential. In the course of doing your job, you may also find that Patients speak to you about their condition or the condition of another Patient that they get to know during therapy. Although there is nothing wrong with this, you must remember that they trust you to keep what they tell you confidential. If they ask you about the status of another Patient, please remind them that this information is confidential. Always remind the Patient that he/she can discuss his/her questions and concerns with the Patient directly.

What Are the Patient's HIPAA Rights?

Each Patient has certain rights under the HIPAA regulations. Unless the information is for treatment, payment, and Health Care Operations, or otherwise required or permitted by law, we cannot release any information without a written authorization from the Patient's Personal Representative since all of our Patients are minors. The Personal Representative must also give you verbal/written permission to discuss information with family members. We must document permission in the Patient's chart. The Patient's Personal Representative also has the following rights:

- To inspect and copy the Patient's medical record.
- To amend the medical record if he/she feels it is incomplete or incorrect.
- To an accounting of all disclosures that were made, and to whom, with certain exceptions.
- To restrict or limit use or access to medical information by others.
- To confidential communications in the manner he/she requests.
- To receive a copy of Covered Entity's Notice of Privacy Practices.

If the Patient or a Personal Representative feels Covered Entity or its Workforce has not followed the HIPAA regulations, the Patient can make a formal, written complaint to Covered Entity's Privacy Officer or to HHS.

What are Ways to Protect Confidentiality?

a. Spoken Communications

- Watch what you say, where you say it, and to whom.
- Speak in a quiet voice when you share information.
- Close doors when discussing private information.
- Do not talk about health information matters in front of others.
- If someone asks you a question involving personal information, make sure that person has a "need to know" before answering.
- Do not share any PHI on Children's TherAplay clients outside of our clinic. Do not give yourself permission to speak about any client even if you believe the parent won't care.

b. Telephone Communications

- Never leave personal health information on an answering machine regarding a Patient's conditions, therapy, or progress in therapy.
- If you are leaving a message on an answering machine/voice mail, only leave the name of the person calling and Covered Entity's telephone number with your contact phone number and request a call back.
- Do not leave messages with anyone other than the Personal Representative or designee of the Personal Representative.

c. Medical Records

- Make sure medical records are only available to individuals who need to see them.
- Store them in an area not easily accessible to non-essential members of the Workforce.
- Do not take medical records home or out of the office unless necessary for a work related purpose and only if those medical records are stored on a secured device issued by Children's TherAplay. The secured device should be kept in a secure spot at all times and not left unattended, such as on a car seat.

- Do not leave medical records lying around unattended or in an area where others can see them.

- Return the medical record to its appropriate location when finished viewing it.

d. Trash

- Shred all papers containing personal health information.

- Put trash cans and shredders as close as possible to fax machines and desks where personal health information is used.

- If you see un-shredded paper discarded in a trash can, remove it and bring it to your supervisor.

e. Fax Transmissions

- Do not leave papers containing private health information on the fax machine unattended.

- If possible, notify the receiver when you are sending a fax.

- Have a fax cover sheet with a statement that the fax contains protected health information, re-disclosure is strictly prohibited, and what to do if the wrong person gets it.

f. Computers

- Use your own personal user ID and a "strong" password which is not a guessable name and change it as instructed.

- Never share your password or write down your password except with your supervisor.

- Position your monitor so it is not facing where someone that is not otherwise permitted could view identifiable health information.

- Never leave a computer unattended without logging off.

- All e-mails sent, which contain identifiable health information, should be encrypted and the sender/receiver should be authenticated.

- Double-check the address before sending any e-mail.

- Never remove/discard computer equipment, disks, or software without your supervisor's permission.

- Always use a screen saver that automatically locks your screen after five minutes if you do not use your computer or walk away from your computer during that time period.

- Install an anti-virus software program.

Short List of Examples of HIPAA Violations

The following is a short list of examples (there are many more …) of different types of HIPAA violations:

a. An inappropriate conversation regarding a particular patient that take place in a public area;

b. Posting a photograph of a Patient receiving therapy or with one of our horses on your personal social media page;

c. Posting a photograph of a Patient receiving therapy or with one of our horses on the Covered Entity's Social Media Page without receiving an Authorization and following all other requirements of the Covered Entity.

d. Commenting on a Patient's or their parents social media page and identifying the fact that the Patient receives therapy at the Covered Entity.

e. A careless error which causes Covered Entity to send a fax or other regular mail containing PHI to a third party who has no "need to know" this information;

f. Taking a laptop, CD/DVD or paper copies of Covered Entity medical records off premises, even if for a legitimate business purpose, and leaving them in an unsecured location (e.g., an unlocked car, public place, home) where they can be accessed by persons who have no "need to know" this information whatsoever;

g. Sending PHI to a third party by e-mail that has not been encrypted in accordance with Covered Entity security requirements;

h. Gaining access to any PHI maintained by Covered Entity, that pertains to an individual for whom you are not personally involved in the individual's treatment, either out of curiosity because the patient is a "VIP", or alternatively, in response to a request from a neighbor or friend who requested the information from you;

i. Discarding PHI or otherwise placing PHI in the trash without complying with Covered Entity policy which requires proper shredding or other destruction;

j. Sharing your user ID and/or password necessary to access PHI maintained by Covered Entity, a hospital, surgery Covered Entity or other health care organization with another person, whether another Covered Entity personnel or other third party;

k. Selling or otherwise disclosing PHI regarding an individual for personal or financial gain or other unlawful or malicious purposes;

l. Discussing or otherwise posting PHI regarding an individual on any Facebook, LinkedIn, Twitter or other social media account.

If you have any questions or concerns regarding how Patient information is used, disclosed or safeguarded, contact your supervisor or the Privacy/Security Officer.

Attachment 3
HIPAA TRAINING CERTIFICATION FORM

I hereby acknowledge and agree that as a condition of my work relationship or volunteering with Covered Entity:

1. I have attended Covered Entity's HIPAA Privacy and Security Training Program and have been given the opportunity to ask questions.

2. I understand that I have reviewed Covered Entity's Protected Health Information Privacy and Security Policies and I understand that any updates and changes will be made available to me from time to time by my supervisor.

3. I agree to comply with these Policies at all times while working for or volunteering for Covered Entity.

4. I agree to maintain the privacy and security of any and all protected health information of Covered Entity's Patients at all times, even after my relationship with Covered Entity has terminated or otherwise expired.

5. I understand that if I fail to comply with these Policies:

    A. I am at risk of disciplinary or other corrective action by Covered Entity up to and including termination of my work relationship with Covered Entity; and

    B. I may be personally at risk of civil or criminal penalties pursuant to applicable laws and regulations, including but not limited to the Health Information Portability and Accountability Act of 1996 ("HIPAA") and certain privacy and security regulations promulgated hereunder.

_____

Printed Name:

_____ _____

Signature Date

Attachment 4
WORKFORCE CONFIDENTIALITY AGREEMENT

DATE: _____

PRINT FULL NAME OF WORKFORCE MEMBER HERE: _____

1. **Definitions**. For purposes of this Agreement, the following capitalized terms are defined as follows:

   a. **Access** means any action taken to read, write, modify, transmit, disclose, discuss, store, maintain, transport, destroy or otherwise access Confidential Information or Electronic Media, as appropriate, for any purpose.

   b. **Applicable Requirements** means all applicable laws, regulations and the then-current policies, procedures, standards and other requirements of Covered Entity, including, but not limited to, requirements arising under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

   c. **Confidential Information** means any and all confidential, proprietary, privileged or otherwise protected information that has a special and unique nature and value to Covered Entity. This Confidential Information shall include, but not be limited to, oral, observed, written, or electronic information, including, but not limited to, individually identifiable information of patients, including Protected Health Information or "PHI" protected by HIPAA, confidential information of employees, other personal, non-public information, and other proprietary information maintained by or on behalf of Covered Entity through the use of Electronic Media or any other medium, including paper and files.

   d. **Electronic Media** means any computers, workstations, laptops, tablets, smart phones, facsimile and/or scanning equipment, MP3 or "jump" drives, CDs, DVDs, e-mail (whether Covered Entity's Intranet or personal e-mail), text messages or other software or applications that may be used to Access Confidential Information, whether on or off duty or on or off Covered Entity premises.

   e. **Workforce** means any employee, leased employee, contract agency staff, Licensed Health Professional student, volunteer or any other person whose conduct, in the performance of their duties, would be under the direct supervision and control of Covered Entity, whether compensated or not.

2. **Agreement.** I am the above-named person and as a member of Covered Entity's Workforce, I hereby acknowledge and agree that:

   a. I will comply with all Applicable Requirements that govern Access to Confidential Information. I will also protect the privacy and security of all Confidential Information at all times. If I Access Confidential Information that I am not authorized to Access or if I violate any Applicable Requirements, I agree to immediately notify Covered Entity.

b. I will Access Confidential Information only for authorized purposes that permit me to perform my assigned duties but only on a "need to know" basis in accordance with those "minimum necessary" standards adopted by Covered Entity and required under HIPAA.

c. I understand that not all of the Workforce is authorized to Access a subset of Confidential Information through the use of Electronic Media that is owned by Covered Entity. If I am so authorized, I will comply with all Applicable Requirements.

d. I understand that only specially authorized Workforce is permitted to Access Confidential Information through the use of Electronic Media that is their own personal property, such as their mobile phone or personal computer. If Workforce does utilize Confidential information on their personal Electronic Media, such as texting on a cell phone, the text must be written in such a way where the patient cannot be identified. If I am so authorized by the Privacy Officer/Security Officer or designee, I will comply with all Applicable Requirements.

e. Regardless of how I Access Confidential Information and/or Electronic Media, I will comply with all Covered Entity's policies governing usernames, passwords, multi-factor authentication, automatic logoffs, downloads, use of the Intranet, encryption in transit, encryption at rest, and on and off-premises security safeguards. I recognize that any means of access granted to me by Covered Entity (e.g., username, password, multi-factor authentication) has been assigned to me alone unless prior authorization has been received from the Privacy/Security Officer. I may not share such means of access with any other person, even if that individual has also been granted access by Covered Entity. I agree that I am fully responsible for protecting any passwords, usernames, or multi-factor authentication methods assigned to me. If I become aware of any other person using my access information, including passwords, username or multi-factor authentication method, I will immediately report that to Covered Entity.

f. I have no expectation of privacy in connection with my Access to Confidential Information and any Electronic Media that is owned by Covered Entity. I understand that any use of Electronic Media or Confidential Information that is offensive, disruptive, harassing, fraudulent or illegal is strictly prohibited. Given these considerations, I hereby give my express consent to Covered Entity to monitor, modify, or remove my Access to Confidential Information and any Electronic Media that is owned by Covered Entity without giving me any other formal notice of said monitoring.

g. Prior to any termination or other expiration of my employment or other affiliation with Covered Entity, I agree to return any and all Confidential Information and any Electronic Media owned by Covered Entity, that may be in my personal possession, to my supervisor. In addition, if I have Accessed Confidential Information through the use of Electronic Media that is my own personal property, regardless of whether such Access was authorized by the Privacy Officer/Security Officer, prior to any termination or other expiration of my employment or other affiliation with Covered Entity, I will promptly cooperate and allow the Privacy Officer/Security Officer, or designee, to examine the applicable Electronic Media and remove any Confidential Information or records of Confidential Information on the Electronic Media.

3. **Violations.** I acknowledge that any unauthorized Access to Confidential Information or Electronic Media owned by Covered Entity is a serious violation and shall result in prompt

investigation and disciplinary action including, but not limited to, termination of my employment or other relationship with Covered Entity. I also acknowledge and agree that any unauthorized Access to Confidential Information or Electronic Media may require Covered Entity to notify certain persons or entities in accordance with Applicable Requirements, any of which may result in further civil (lawsuit, civil money penalties), criminal (fines and imprisonment) or administrative actions (licensure revocation or suspension, Federal program exclusion) for which I will be solely responsible. Pursuant to 18 USC § 1833(b), I understand I may not be held criminally or civilly liable under any federal or state trade secret law for disclosure of Covered Entity's trade secrets: (i) made in confidence to a government official, either directly or indirectly, or to an attorney, solely for the purpose of reporting or investigating a suspected violation of law; and/or (ii) in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. Additionally, if I sue Covered Entity for retaliation based on the reporting of a suspected violation of law, I may disclose a trade secret to my attorney and use the trade secret information in the court proceeding, so long as any document containing the trade secret is filed under seal and I do not disclose the trade secret except pursuant to court order.

4. **Effective Date; Amendments**. This Agreement shall remain in effect both during and following any termination or other expiration of my employment or other affiliation with Covered Entity, for any reason, in order to safeguard all Confidential Information and Electronic Media and to protect the resources, relationships and reputation of Covered Entity.

I have been provided with a copy of this Agreement which I have read, understood, signed and agreed to comply with in all respects and at all times.

Signature_____ Date_____

Attachment 5
ACTION FORM

This Action Form Concerns Facts, Event or Complaint Related to (Check All That Apply):
___ Privacy ___ Security ___ Other [Explain] _____

Date Form Completed: _____ Person Completing Form: _____

Description of Facts, Event or Complaint Resulting in this Action Form (Describe in full; attach copy of any related documents; attach additional pages if necessary):

_____

_____

_____

_____

Person(s) Involved: (Check all that apply and describe contact information for all persons involved below; attach additional pages if necessary)

___ Employee/Staff/Volunteer ___ Patient/Family/Friend ___ Business Associate ___ Other

_____

_____

_____

_____

_____

[ONLY PRIVACY/SECURITY OFFICER MAY WRITE BELOW THIS LINE]

_____ Date Investigation Completed by Privacy/Security Officer

_____ Date of Written Report to _____and/or Legal Counsel Summarizing Complaint, Investigation and Recommended Actions (Attach Complete Copy)

_____ Date of Action by _____(Attach Documentation of Any Actions Taken)

ORIGINAL (w/attachments.): File No. -_____
COPY (w/o attachments): Privacy/Security Officer Complaint/Incident Log Book

This document, prepared in anticipation of litigation at the advice of counsel, is privileged and confidential and subject to the attorney-client privilege and work product doctrine.

Attachment 6
PRIVACY/SECURITY FLOW SHEET

Date	Description of Event	Document(s) Filed	Signature
	Privacy Notice to Patient		

ALL ORIGINALS: Filed Under Privacy Tab in Patient Record (Chronological Order)

Attachment 7
HIPAA RISK ASSESSMENT FORM

Date(s) of Incident/Disclosure	
Date(s) of Discovery	
Date Reported to Investigator	
Investigator	
Person(s) Involved (Patient, Employee, Other)	
Detailed Incident Summary	
Breach Excludes [*42 CFR §164.402(1)*]	Breach excludes: ☐ (i) Any unintentional acquisition, access, or use of PHI by a workforce member (or person acting under authority of CE or BA) if made in good faith and within the scope of authority and does not result in any further use or disclosure ☐ (ii) Any inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at same CE or BA or organized health care arrangement and the PHI is not further used or disclosed ☐ (iii) A disclosure of PHI where a CE or BA has good faith believe that unauthorized person to who disclosure was made would not reasonably have been able to retain such information
Risk Assessment [*45 CFR §164.402(2)*]	Based on a review of the facts, it appears **there is a low/high probability that the protected health information has been compromised**. Our conclusion is based on the following: (i) The nature and extent of the protected health information involved, including types of identifiers and the likelihood of re-identification (i.e. does it pose a significant risk of financial, reputational or other harm): (ii) The unauthorized person who used the protected health information or to whom the disclosure was made: (iii) Whether the protected health information was actually acquired or viewed: (iv) The extent to which the risk to the protected health information has been mitigated:
Corrective Action	
HIPAA/ Department of Health and Human Reporting Obligations	☐ No Breach: ☐ Yes Breach: Date Reported to Patient(s): _____ Date Reported to DHHS: _____ Date Reported to Media:_____ (>500 only)
Other State/Federal Reporting Requirement	

Attachment 8
DECISION TREE
IN ORDER TO DETERMINE
ANY HIPAA BREACH NOTIFICATION OBLIGATIONS

#1. Was there a Breach, which is defined to be an unauthorized acquisition, access, use or disclosure of that compromises the Privacy of PHI (in any form or medium) or the Security of ePHI? [1] Examples of a Breach may include:

- An inappropriate conversation regarding a Covered Entity patient that takes place in a public area.

- A careless error by a Covered Entity representative which causes a fax or other regular mail containing PHI to a third party who has no "need to know" this information whatsoever.

- Taking PHI or any Electronic Media which contains ePHI off Covered Entity premises, even if for a legitimate business purpose, and leaving the PHI/ePHI in an unsecured location (e.g., an unlocked car, public place, home) where the PHI/ePHI can be accessed by persons who have no "need to know" this information whatsoever.

- Sending PHI to a third party by e-mail, using an AOL, Yahoo, Gmail or other Internet account, that has not been encrypted in accordance with Covered Entity policies.

- Gaining access to any PHI regarding an individual Covered Entity patient when you have absolutely no reason or "need to know" this information.

- Discarding PHI or otherwise placing PHI in the trash without complying with Covered Entity policies which requires proper shredding or other destruction.

- Sharing your Covered Entity user ID and/or password with another person, whether a Covered Entity representative or other third party.

- Selling or otherwise disclosing PHI or ePHI regarding an individual Covered Entity patient for personal or financial gain or other unlawful or malicious purposes.

- Posting pictures of minor Patients receiving therapy on your personal social media page, such as Facebook.

[1] *See* definition of "breach" at 45 C.F.R. § 164.402.

Option A: If the Privacy/Security Officer conducts an investigation and determines there is evidence of a Breach, a HIPAA accounting must be completed in accordance with current HIPAA Policy. Additionally, go to #2.

Option B: If the Privacy/Security Officer conducts an investigation and determines there is no evidence of a Breach, the Privacy/Security Officer should document these findings in the investigation file to confirm that no obligation to notify patient under HIPAA is required. STOP.

#2. Did the Breach involve the disclosure of Unsecured PHI or ePHI that was not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS?[2]

Option A: If the Privacy/Security Officer conducts an investigation and determines there is evidence of a Breach that Unsecured PHI or EPHI was involved, go to #3.

Option B: If the Privacy/Security Officer conducts an investigation and determines there is no evidence that Unsecured PHI or ePHI was involved, the Privacy/Security Officer should document these findings in the investigation file to confirm that no obligation to notify patient under HIPAA is required. STOP.

#3. Does the Breach involve Unsecured PHI that qualifies as one of the three exceptions under HIPAA[3], either because:

- The Breach was an unintentional acquisition, access or use of PHI by Workforce or other individual acting under the authority of the Covered Entity, or Business Associate, and made in good faith and within the course and scope of employment or other professional relationship, as appropriate, and the PHI is not further acquired, accessed, used, or disclosed by any person (Example: billing employee inadvertently accesses PHI about wrong patient in the performance of job duties and promptly exits from system)?

Option A: If the Privacy/Security Officer conducts an investigation and determines that this exclusion does not apply, go to #4.

Option B: If the Privacy/Security Officer conducts and investigation and determines that this exclusion does apply, the Privacy/Security Officer should document these findings in the investigation file to confirm that no obligation to notify patient under HIPAA is required. STOP.

OR

- The Breach was an inadvertent disclosure of PHI by Workforce or other individual acting under the authority of the Covered Entity or a Business Associate to another similarly situated Workforce or individual and the PHI is not further acquired, accessed, used or disclosed by any person (Example: Billing employee receives PHI about a patient mistakenly sent by a nurse; billing employee notifies nurse of misdirected PHI and deletes same).

[2] *See* definition of "unsecured protected health information" at 45 C.F.R. § 164.402.
[3] *See* definition of "breach" at 45 C.F.R. § 164.402.

Option A: If the Privacy/Security Officer conducts an investigation and determines that this exclusion does not apply, go to #4.

Option B: If the Privacy/Security Officer conducts an investigation and determines that this exclusion does apply, the Privacy/Security Officer should document these findings in the investigation file to confirm that no obligation to notify patient under HIPAA is required. STOP.

OR

- The Breach was an inadvertent disclosure of PHI by Workforce or other individual acting under the authority of the Covered Entity or a Business Associate to a third party and there is a good faith belief that the recipient would not have been reasonably able to retain the PHI (Example: EOB sent to wrong patient and returned by post office, unopened and undeliverable).

Option A: If the Privacy/Security Officer conducts an investigation and determines that this exclusion does not apply, go to #4.

Option B: If the Privacy/Security Officer conducts an investigation and determines that this exclusion does apply, the Privacy/Security Officer should document these findings in the investigation file to confirm that no obligation to notify patient under HIPAA is required. STOP.

#4. If the Privacy/Security Officer conducts an investigation under #1 – #3 and determines there is evidence of a Breach involving Unsecured PHI or ePHI, the acquisition, access, use, or disclosure of Unsecured PHI or ePHI is presumed to be a breach unless the Privacy/Security Officer determines that there is a "low probability" that the Unsecured PHI or ePHI has been compromised.[4] This evaluation is conducted by the Privacy/Security Officer before making any final determination whether Covered Entity has an obligation to the notify patient under HIPAA. The risk evaluation of "low probability" of compromise turns on an examination of the following four (4) factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the PHI or to whom the disclosure was made;
(iii) Whether the PHI was actually acquired or viewed; and
(iv) The extent to which the risk to the PHI has been mitigated.[5]

Examples of "low probability of compromise" may include any of the following:

- If Covered Entity misdirects a fax containing PHI to the wrong provider, and upon receipt, the receiving provider Covered Entity calls Covered Entity to say it has received the fax in error and has destroyed it.

[4] *See* definition of "breach" at 45 C.F.R. § 164.402.
[5] *See* definition of "breach" at 45 C.F.R. § 164.402.

- Breach did not include any of the 16 limited data set identifiers listed in 45 CFR §164.514(e)(2) nor the zip code or date of birth of the patient.

- Breach did not include any De-Identified PHI that was at risk of being Re-Identified.

- PHI was received and/or used by another Covered Entity or Business Associate covered by HIPAA.

- PHI was received by a third party and returned with evidence that the privacy and security of the PHI was not compromised (e.g. lost laptop that is recovered and subjected to forensic analysis to confirm same; mail sent to an incorrect addressee returned unopened).

Option A: If the Privacy/Security Officer conducts the risk assessment and determines that the Breach involved Unsecured PHI which represents "low probability of compromise" to the patient, the Privacy/Security Officer should document these findings in the investigation file to confirm that no obligation to notify patient under HIPAA is required. STOP.

Option B: If the Privacy/Security Officer conducts the risk assessment and determines that the Breach involved Unsecured PHI which does not represent "low probability of compromise", the Privacy/Security Officer should document these findings in the investigation file to confirm that Covered Entity must notify patient under HIPAA in accordance with instructions set forth under #5 below. STOP.

#5. If the Privacy/Security Officer conducts an investigation, in addition to a risk assessment, and determines that Covered Entity must notify patient under HIPAA, the Privacy/Security Officer shall refer to Attachments 7 and 8 to these Policies in addition to consulting with legal counsel to confirm any and all patient, HHS, Attorney General or other notification obligations that apply under HIPAA.

Attachment 9
NOTIFICATION REQUIREMENTS UNDER INDIANA LAW FOR AN UNAUTHORIZED ACCESS TO PERSONAL INFORMATION

#1. Was there an Unauthorized Access? An Unauthorized Access is defined under Indiana law as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Personal Information maintained by Covered Entity. This definition also includes any computerized data transferred to another medium (e.g., paper, microfilm, etc.) even if transferred data no longer exist in computerized format. "Personal information" of customers means: (1) a social security number that is not Encrypted or Redacted; or (2) an individual's first and last names, or first initial and last name AND one or more of the following numbers that are not Encrypted or Redacted: (i) driver's license; (ii) state ID card; or (iii) credit card, financial account or debit card plus the necessary code to access the account. An Unauthorized Access does not include: (1) the good faith acquisition of Personal Information by an employee or agent of Covered Entity for lawful purposes; or (2) unauthorized acquisition of a portable electronic device containing Personal Information if the device is Encrypted.

Examples of an "Unauthorized Access" include, but are not limited to the following:

- Discarding Personal Information or otherwise placing Personal Information in the trash without complying with Covered Entity policies which requires proper shredding or other destruction; or

- Selling or otherwise disclosing Personal Information regarding an individual Covered Entity Patient for personal or financial gain or other unlawful or malicious purposes.

Option A: If the Privacy/Security Officer conducts an investigation and determines there is evidence of an Unauthorized Access, a HIPAA accounting must be completed in accordance with current HIPAA Policy, if applicable. Additionally, go to #2.

Option B: If the Privacy/Security Officer conducts an investigation and determines there is absolutely no evidence of an Unauthorized Access, the Privacy/Security Officer should document these findings in the investigation file to confirm that no obligation to notify Patient under applicable state law.

#2. Was the Personal Information Redacted or Encrypted? Under Indiana law, Personal Information is "Encrypted" if it has been: (1) transformed through the use of an algorithmic process into a form that has low probability of meaning without use of confidential process or key; or (2) secured by another method that renders the Personal Information unreadable or unusable. Personal Information is "Redacted" if it only includes the last four (4) digits of a number, or, in the case of a social security number, the last five (5) digits.

Option A: If the Privacy/Security Officer conducts an investigation and determines there is evidence of an Unauthorized Access to Personal Information that was not Redacted or Encrypted, go to #3.

Option B: If the Privacy/Security Officer conducts an investigation and determines that the Personal Information was Redacted or Encrypted, the Privacy/Security Officer should document these findings in the investigation file to confirm that Patient notification under applicable state law is not required.

#3. If the Privacy/Security Officer conducts an investigation, and determines that Covered Entity must notify Patients under applicable state law, the Privacy/Security Officer shall consult with legal counsel to confirm any and all Patient, Attorney General, or other notification obligations that apply.

Attachment 10
HIPAA AND STATE LAW REQUIREMENTS GOVERNING PATIENT NOTIFICATIONS IN THE CASE OF A HIPAA BREACH OR OTHER UNAUTHORIZED ACCESS TO PERSONAL INFORMATION GOVERNED BY STATE LAW

I. HIPAA

The following is a summary of the HIPAA notification obligations that are mandated in the event of a Breach involving Unsecured PHI.

Notification to Individuals

Under HIPAA, Covered Entity is required to notify individuals whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a security breach. Notification of the Breach must be made without unreasonable delay, but no later than sixty (60) calendar days after discovery of the Breach. A Breach shall be treated as discovered by Covered Entity as of the first day such Breach is known to Covered Entity, or by exercising reasonable diligence, would have been known to Covered Entity.

Notification to the Media

If a Breach involves PHI of more than five hundred (500) individuals in a state, Covered Entity must give notice of the Breach to prominent media outlets, such as a major television station or newspaper. Notification of the Breach must be made without unreasonable delay, but no later than sixty (60) calendar days after discovery of the Breach.

Notification to the Secretary of HHS

For Breaches involving five hundred (500) or more individuals, Covered Entity shall provide notification to the Secretary of HHS concurrently with its notification to individuals, without unreasonable delay, and no later than sixty (60) calendar days after discovery of the Breach. Such reporting shall be made in the manner specified on the HHS website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.
If fewer than five hundred (500) individuals are affected, Covered Entity must maintain a log or other documentation of such Breaches, and not later than sixty (60) days after the end of the calendar year, provide such information to the Secretary of HHS in accordance with the manner specified on the HHS website at:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

Notice Requirements

All Notices must include, if possible, the following information:

- A brief description of what happened, including the dates of the Breach and the date of the discovery of the Breach;
- A description of the types of unsecured PHI that were involved in the Breach;
- Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
- A brief description of what Covered Entity is doing to investigate the Breach, to mitigate losses, and protect against further Breaches; and
- Contact procedures, including toll-free telephone number, e-mail address, web site, or postal address, for individuals to ask questions or learn additional information.

The Notice to individuals must be:

- In writing to individual by mail (or e-mail, if individual agrees to electronic notice);
- Sent to last known address of individual; and
- If insufficient or out-of-date contact information is available, Covered Entity must give notice in substitute form, such as a posting on Covered Entity website, or notice in major print or broadcast media.

II. State Law

The following is a summary of the Indiana law notification obligations that are mandated in the event of an Unauthorized Access to Personal Information.

Under Indiana law, upon notice or discovery of any Unauthorized Access of Personal Information Breach, Covered Entity must notify all Indiana Patients whose Personal Information was or may haven the subject of the Unauthorized Access without unreasonable delay. Any Unauthorized Access involving more than 1,000 Indiana Patients also requires disclosure to each consumer credit reporting agency (as defined in 15 U.S.C. 1681a(p)), of the information necessary to assist the consumer reporting agency in preventing fraud. In addition, Covered Entity is required to report the Unauthorized Access to the Indiana Attorney General's office.

Under Indiana law, Covered Entity must provide notice of the Unauthorized Access to the affected individuals using one (1) of the following methods: (1) mail; (2) telephone; (3) facsimile (fax); or (4) electronic mail. If the Unauthorized Access involves more than five hundred thousand (500,000) Indiana Patients, or if Covered Entity determines that the cost of the disclosure will be more than $250,000, Covered Entity may elect to make the notification by using both of the following methods: (1) conspicuous posting of the notice on Covered Entity website; and (2) notice to major news reporting media in the geographic area where Indiana Patients affected by the Unauthorized Access reside.

Attachment 11
PATIENT REQUEST TO RESTRICT PHI USES AND DISCLOSURES FORM

I hereby authorize The Children's TherAplay Foundation (the "Covered Entity") to acknowledge that I am my child is a Patient, but I ask that no other information is provided to individuals who inquire about my health status, my telephone number, or other personal information. Instead, I ask that Covered Entity request the inquiring individual's full name and contact information and provide it to me with the understanding that I will respond to the individual's inquiry if I so choose. Additionally, I ask Covered Entity to honor the following restrictions regarding the use or disclosure of my child's protected health information ("PHI"):

(Please check only those boxes that apply and describe the nature of the requested restriction; use extra pages if necessary; cross out any boxes that do not apply at this time):

_____ Please do not disclose any PHI to my health benefits plan related to the services and dates of service designated below on the condition that I agree to pay for all such services, in full, on the date of service:

Description of Service: _____

Date(s) of Service: _____

Note: This request may be approved only in accordance with health benefit plan requirements.

To be completed by Privacy/Security Officer: _____ Accepted _____ Denied

_____ Please do not disclose any of my PHI to any of the following individuals without my prior express written authorization:

_____

_____

_____

_____

To be completed by Privacy/Security Officer: _____ Accepted _____ Denied

_____ Please do not contact the following "next of kin" listed on my Authorization for Disclosure of Protected Health Information with any PHI or other information regarding my health status or treatment, except in the case of an emergency:

_____

_____

_____

_____

To be completed by Privacy/Security Officer: _____ Accepted _____ Denied

_____ Please provide me with communications of protected health information only by the following means or at the following locations:

To be completed by Privacy/Security Officer: _____ Accepted _____ Denied

_____ Other Request as Specified:

To be completed by Privacy/Security Officer: _____ Accepted _____ Denied

_____

Patient or Personal Representative* Signature, Printed Name, Date Completed

(*) If signed by Personal Representative, state relationship to Patient:_____

_____

Privacy/Security Officer's Signature, Printed Name, Date Completed

ORIGINAL: In Patient Record Under Privacy Tab
COPY: To Patient or Personal Representative

Attachment 12
Authorization for the Disclosure of Protected Health Information on Social Media

1. Child's Name: _____ Parent/Guardian's: Name: _____

2. By signing below, I hereby authorize my child's Protected Health Information to be disclosed. The Protected Health Information I am authorizing for disclosure is the following:

   ❑ "Standard" release of all information maintained by Children's TherAplay Foundation, Inc. (Includes evaluation, daily therapy notes and progress notes, etc.)
   ❑ Specific information from my child's chart: My child's name; child's photo or videos while receiving therapy or other services at Children's TherAplay; and, information related to my child's progress, goals, and treatment (excluding copies of evaluations, notes, and records), including content that was created or existed before, on or after the date of the HIPAA Authorization.

3. The person or group of people who are authorized to disclose my child's Protected Health Information are as follows: The Children's TherAplay Foundation, Inc.

4. I hereby request The Children's TherAplay Foundation, Inc. to disclose my child's Protected Health Information to the following person(s) or institutions(s):
   ♦ Name of person or parties to receive your child's medical information:
   The information may be disclosed on Children's TherAplay's website, social media, paper and digital publications, press-releases and other web-based platforms. The information may also be disclosed to Children's TherAplay board of directors, volunteers, and donors.

   ♦ Please indicate where we should mail your child's medical information (or any alternative instructions for delivery): N/A

5. This authorization will expire 60 days from signing, unless an alternative date is indicated: Until such time as the child is no longer receiving services at Children's TherAplay.

6. The purpose of this disclosure is as follows: To allow Children's TherAplay to use the information for promotional, marketing, fundraising, training, and other related purposes. Children's TherAplay will not receive remuneration or payment for any disclosure of my child's protected health information.

7. I understand that I have the right to revoke this Authorization, if the revocation is in writing, at any time by sending a written request to The Children's TherAplay Foundation, 9919 Towne Road, Carmel, IN 46032. I am aware that my revocation will not be effective regarding the uses and disclosures of content by Children's TherAplay made in reliance on this HIPAA Authorization and that have been made prior to receipt of my revocation.

8. I understand that The Children's TherAplay Foundation, Inc. may not condition treatment, payment, enrollment or eligibility for benefits on whether I sign this authorization.

9. I understand that my child's Protected Health Information that is disclosed under this Authorization may be subject to re-disclosure by the recipient, and the privacy of my child's Protected Health Information will no longer be protected by the law.

10. I understand that if I am requested to sign this Authorization by The Children's TherAplay Foundation, Inc., that (i) I will be given a copy of this Authorization; (ii) I may inspect or copy the information to be used or disclosed; and (iii) I may refuse to sign this Authorization.

    By signing this Authorization, I acknowledge that I have read and understand this Authorization. Further, I authorize the disclosure of my child's Protected Health Information in accordance with the terms of this Authorization.

_____	_____
Signature of Parent or Guardian	Signature of Parent or Guardian
_____	_____
Date	Date

Attachment 13
AUTHORIZATION FOR THE DISCLOSURE OF PROTECTED HEALTH INFORMATION

1. 1. Child's Name: _____ Parent/Guardian's: Name: _____

2. By signing below, I hereby authorize my child's Protected Health Information to be disclosed. The Protected Health Information I am authorizing for disclosure is the following:

   ❑ "Standard" release of all information maintained by Children's TherAplay Foundation, Inc. (Includes evaluation, daily therapy notes and progress notes, etc.)
   ❑ Specific information from my child's chart: _____

3. The person or group of people who are authorized to disclose my child's Protected Health Information are as follows: The Children's TherAplay Foundation, Inc.

4. I hereby request The Children's TherAplay Foundation, Inc. to disclose my child's Protected Health Information to the following person(s) or institutions(s):
   ♦ Name of person or parties to receive your child's medical information:
   _____

   ♦ Please indicate where we should mail your child's medical information (or any alternative instructions for delivery, such as email or fax): _____

5. This authorization will expire 60 days from signing, unless an alternative date is indicated: _____

6. The purpose of this disclosure is as follows: _____

7. I understand that I have the right to revoke this Authorization, if the revocation is in writing, at any time by sending a written request to The Children's TherAplay Foundation, 9919 Towne Road, Carmel, IN 46032. I am aware that my revocation will not be effective regarding the uses and disclosures of content by Children's TherAplay made in reliance on this HIPAA Authorization and that have been made prior to receipt of my revocation.

8. I understand that The Children's TherAplay Foundation, Inc. may not condition treatment, payment, enrollment or eligibility for benefits on whether I sign this authorization.

9. I understand that my child's Protected Health Information that is disclosed under this Authorization may be subject to re-disclosure by the recipient, and the privacy of my child's Protected Health Information will no longer be protected by the law.

10. I understand that if I am requested to sign this Authorization by The Children's TherAplay Foundation, Inc., that (i) I will be given a copy of this Authorization; (ii) I may inspect or copy the information to be used or disclosed; and (iii) I may refuse to sign this Authorization.

By signing this Authorization, I acknowledge that I have read and understand this Authorization. Further, I authorize the disclosure of my child's Protected Health Information in accordance with the terms of this Authorization.

_____ _____

Signature of Parent or Guardian Signature of Parent or Guardian

_____ _____

Date Date

Attachment 14
NOTICE OF PRIVACY PRACTICES

[see attached]

THE CHILDREN'S THERAPLAY FOUNDATION, INC.

NOTICE OF PRIVACY PRACTICES

THIS NOTICE OF PRIVACY PRACTICES ("NOTICE") DESCRIBES HOW MEDICAL INFORMATION ABOUT YOUR MINOR CHILD MAY BE USED AND DISCLOSED, HOW YOU CAN GET ACCESS TO THIS INFORMATION, YOUR RIGHTS CONCERNING YOUR CHILD'S PROTECTED HEALTH INFORMATION ("PHI") AND OUR RESPONSIBILITIES TO PROTECT YOUR CHILD'S PHI.

HOW WE USE AND RELEASE YOUR PHI?

We primarily maintain your child's PHI in a secure electronic format. Your child's PHI will most often be used, shared, or disclosed electronically. The following section explains some of the ways we are permitted to use and release your child's PHI without authorization from you.

TREATMENT PURPOSES

While we are providing your child with therapy services, we may need to share your child's PHI with other health care providers or other individuals who are involved in your child's treatment.

Examples include: doctors, hospitals, pharmacists, therapists, nurses, and labs that are involved in your child's care.

PAYMENT PURPOSES

We may need to share a limited amount of your child's PHI to obtain or provide payment for the health care services provided to your child.

HEALTH-CARE OPERATIONS PURPOSES

We may need to share your child's PHI in the course of conducting health care business activities that are related to providing health care to your child.

Examples include:

- **Quality Improvement Activities** - To use and release PHI to improve the quality or the cost of care. This may include reviewing the treatment and services provided to your child. This information may be shared with those who pay for your child's care, or with other agencies that review this data.

- **Case Management and Referral** - If your child has a health problem or a health care need is identified by you or one of your child's providers, your child may be referred to an organization such as a home health agency, medical equipment company, or other community or government program. This may require the release of your child's PHI to these agencies.

- **Appointment Reminders** - To remind you of recommended services, treatments, or scheduled appointments.

- **Business Associates** - To disclose your child's PHI to Business Associates for services provided through contracts with Business Associates, such as medical transcription services and record storage companies. Business Associates are required by Federal law to protect your PHI.

- **Audits** - To ensure our business practices comply with the law and with our policies. Examples include: audits involving quality of care, medical bills, or patient confidentiality.

OTHER PURPOSES

- **Required By Law** - Sometimes we must report some of your child's PHI to legal officials or authorities, such as law enforcement officials, court officials, governmental agencies, or attorneys. Examples include: reporting suspected abuse or neglect, reporting domestic violence or certain physical injuries, or responding to a court order, subpoena, warrant, or lawsuit request.

- **Public Health Activities** - We may be required to report your child's PHI to authorities to help prevent or control disease, injury, or disability. Examples include: reporting certain diseases, injuries, birth or death information, information of concern to the Food and Drug Administration, or information related to child abuse or neglect.

- **Health Oversight Agencies** - We may be required to release your child's PHI to authorities so they can monitor, investigate, inspect, discipline or license those who work in the health-care system, or for governmental benefit programs.

- **Activities Related to Death** - We may be required to release your child's PHI to coroners, medical examiners and funeral directors so they can carry out their duties related to your child's death. Examples include: identifying the body, determining the cause of death, or, in the case of funeral directors, carrying out funeral preparation activities.

- **Organ, Eye or Tissue Donation** - In the event of your child's death, we may release your child's PHI to organizations involved with obtaining, storing, or transplanting organs, eyes, or tissue to determine your child's donor status.

- **Research Purposes** - At times, we may use or release PHI about your child for research purposes. However, all research projects require a special approval process before they begin, and do not involve in any marketing or sales activity. This process may include asking for your authorization. In some instances, your child's PHI may be used, but your child's identity is protected.

- **To Avoid a Serious Threat to Health or Safety** - As required by law and standards of ethical conduct, we may release your child's PHI to the proper authorities if we believe, in good faith, that such release is necessary to prevent or minimize a serious and/or approaching threat to your child's health or safety or to the health and safety of the public.

- **Military, National Security or Incarceration/Law Enforcement Custody** - We may be required to release your child's PHI to the proper authorities so they may carry out their duties under the law.

- **Persons Involved in Your Care** - In certain situations, we may release PHI about your child to persons involved with your child's care, such as friends or family members, unless doing so would be inconsistent with any prior expressed preference that is known to us. We may also give information to someone who helps pay for your child's care. You have the right to approve such releases, unless you are unable to function, or if there is an emergency.

- **Notification/Disaster Relief Purposes** - In certain situations, we may share your child's PHI with the American Red Cross or another similar federal, state, or local disaster relief agency or authority, to help the agency locate persons affected by the disaster.

- **Directory Information** - Except for emergency situations or when you object, we may share

your child's location and general condition with persons who request information about your child by name, and may share all of your directory information with members of the clergy.

- **To Provide Proof of Immunization** - We will disclose proof of immunization to a school that is required to have it before admitting a student where you have agreed to the disclosure on behalf of your child.

- **HHS Secretary** - We must disclose your child's PHI to the HHS Secretary to investigate or determine our compliance with the HIPAA.

WHEN IS YOUR AUTHORIZATION REQUIRED?

Except for the types of situations listed above, we must obtain your authorization for any other types of releases of your child's PHI.

WHAT ARE YOUR RIGHTS REGARDING YOUR PHI?

- **Right to Receive This Notice of Privacy Practices** - You have the right to receive a paper copy of this Notice at any time.

- **Right to Request Confidential Communications** - You have the right to ask that we communicate your child's PHI to you in different ways or places. For example, you can ask that we only contact you by telephone at work, or that we only contact you by mail at home. We will do this whenever it is reasonably possible. You can find out how to make such a request by contacting us.

- **Right to Request Restrictions** - You have the right to request restrictions or limitations on how your child's PHI is used or released. We have the right to deny your request if it is unreasonable or difficult to administer. However, if you, or a third party on your behalf, have paid for a health care item or service in full, out of pocket, we must honor your request to restrict information from being disclosed to a health plan for purposes of payment or operations. You may obtain information about how to ask for a restriction on the use or release of your information by contacting us.

- **Right to Access** - With a few exceptions, you have the right to review and receive a copy of your child's PHI. Some of the exceptions include:

    - **o** Psychotherapy notes;
    - **o** Information gathered for court proceedings; and
    - **o** Any information your provider feels would cause you to commit serious harm to your child or to others.

To receive a copy of your child's medical records, please call us or submit a request to Children's TherAplay, Attention Clinic Operations Manager. We will provide you with the necessary forms and assistance. We may charge you the labor costs to copy and/or mail your child's medical records to you. If you are denied access to your child's medical records for any reason, we will tell you the reasons in writing. We will also give you information about how you can file an appeal if you are not satisfied with our decision.

- **Right to Amend** - You have the right to ask that our information in your child's medical records be changed if it is not correct or complete. You must provide the reason why you are asking for a change. You may request a change by sending a request in writing to us. We will provide you with the necessary forms and assistance. We may deny your request if:

- **o** We did not create the information;
- **o** We do not keep the information;
- **o** You are not allowed to see and copy the information; or
- **o** The information is already correct and complete.

- **Right to a Record of Releases -** You have the right to ask for a list of releases of your child's PHI by sending a request in writing to us. Your request may not include dates earlier than what is permitted by applicable law. If you request a record of releases more than once per year, we may charge a fee for providing the list. The list will contain only information that is required by law. This list will not include releases for treatment, payment, health care operations or releases that you have authorized.

- **Right to be notified following a breach of unsecured PHI -** You have the right to be notified if we or one of our Business Associates discloses any unauthorized PHI. We will notify you of the breach as soon as possible but no later than sixty (60) days after the breach has been discovered.

WHAT CAN YOU DO IF YOU HAVE A COMPLAINT ABOUT HOW YOUR CHILD'S PHI IS HANDLED?

If you believe that your child's privacy rights have been violated, you may file a complaint with us or with the Department of Health and Human Services' Office for Civil Rights in Baltimore, Maryland. To receive help in filing a complaint, you may contact us. Your child will not be denied treatment or penalized in any way if you file a complaint.

Contact Information:
Children's TherAplay
Attn: Executive Director
9919 Towne Road
Carmel, Indiana 46032

This Notice of Privacy Practices is effective as of December 8, 2021 and may be updated by us at any time.

Attachment 15
ACKNOWLEDGEMENT OF NOTICE OF PRIVACY PRACTICE

Patient Name _____ **Date** _____

Personal Representative Name and Relationship _____

The above Patient came to The Children's TherAplay ("Covered Entity")for services. on the above date. I acknowledge that I am the Patient's Personal Representative and I received a current copy of Covered Entity's Privacy Notice on or before the date listed above.

Signature: _____

Relationship to Patient: _____

For office use only:

A good faith effort was made by Covered Entity personnel to obtain the Patient (or Personal Representative) signature on the Acknowledgement; however no signature was obtained because:

_____ Personal Representative refused to sign.

_____ Personal Representative was unable to sign or initial because:

_____

_____

_____ There was a medical emergency [_____] will attempt to obtain acknowledgment at the next available opportunity).

_____ Other reason(s), described below:

_____

Signature of Covered Entity staff member completing form:

_____

Attachment 16
PATIENT REQUEST TO ACCESS PHI FORM

Patient Name: _____

Date of Request: _____

Date of Birth: _____

Method of Request: (circle one) Written / Verbal*_____

Description of Protected Health Information Requested:

_____

_____

1. This request will terminate sixty (60) days after the date listed below or upon the occurrence of _____, whichever occurs first.

2. I understand that Covered Entity may deny my request if it is permitted to do so by state and federal law.

3. I agree that Covered Entity may provide a summary of the information requested instead of copies of the actual records. I agree to pay Covered Entity all reasonable fees incurred in preparing the summary and providing it to me.

4. I request that the information is delivered to me in (circle one): printed copy / e-mail / other electronic format (specify):_____.

_____ _____
Patient (or Personal Representative*) Signature Date

_____
Printed Name

If signed by Personal Representative, state relationship to Patient: _____

(*) If the Patient requests protected health information verbally rather than in writing, the request will be documented in the Patient's medical record.

ORIGINAL: In Patient Record Under Privacy Tab
COPY: To Patient (or Personal Representative)

DECISION BY LICENSED HEALTH CARE PROFESSIONAL WHEN DENIAL OF ACCESS IS REVIEWED

Name and address of Patient:

_____
_____
_____
_____

Dear _____:

On _____, 20__, you requested review of Covered Entity's denial of access to your protected health information or "PHI."

Covered Entity's reason for denying your request was ***[state the reason].***

Your request for review was referred to **[*insert name of the Health Care Professional who conducted the review*]** on _____, 20__. Please note that this individual did not participate in the original decision to deny access.

At this time, I am writing to notify you that **[*insert name of the Health Care Professional who conducted the* review]** has upheld/reversed the initial denial of access.

[If the denial was reversed, include the following paragraph] Please contact _____ who will arrange for your requested access to occur.

Very truly yours,

_____
Authorized Official

ORIGINAL: Patient (or Personal Representative)
COPY: Patient Record Under Privacy Tab

Attachment 17
PATIENT REQUEST TO AMEND PHI FORM

Name: _____

Date of Birth: _____

Description of Protected Health Information Amendment Requested:

_____

_____

_____

_____

I understand that Covered Entity may deny my request if it is permitted to do so by state and federal law.

_____ _____
Patient (or Personal Representative*) Signature Date

_____
Printed Name

If signed by Personal Representative, state relationship to Patient:
_____

ORIGINAL: In Patient Record Under Privacy Tab
COPY: To Patient (or Personal Representative)

DECISION REGARDING PATIENT REQUEST TO AMEND PHI

Name and address of Patient: _____
_____
_____
_____

On _____, 20__, you requested an amendment of protected health information or "PHI" about you.

The requested amendment is:

_____ Approved (subject to any limitations described here):
_____
_____

_____ Denied (subject to any limitation described here):
_____
_____

The basis for any denial described above is because the PHI that is the subject of the request:

☐ Was not created by [_____]and the originator of the PHI is available to act on your request.

☐ Is not a part of the record maintained, collected, used or disseminated by or for [_____] that qualifies as part of the Patient Record.

☐ Is not a record that would be available for inspection by you.

☐ Is accurate and complete.

You have the right to submit a written statement disagreeing with this denial. If you want to file such a statement, it should (a) be typed or handwritten in blue or black ink; (b) not be longer than 200 words; and (c) be submitted to Covered Entity's Privacy Officer, either by mail or in person. We may prepare a rebuttal to statement of disagreement and if we do, we will furnish a copy to you.

If you do not want to submit a statement of disagreement, you may request that we provide your request to amendment and our denial with any future disclosures by us of the PHI that is the subject of the amendment. If you want to make that request, it should be submitted to Covered Entity's Privacy Officer, in writing.

As stated in our Privacy Notice, you have the right to contact our Privacy Officer at any time if you wish to file a complaint about our privacy policies and procedures or if you believe we have violated your privacy rights. You also have the right to contact the Department of Health and Human Services in Baltimore, Maryland regarding these matters, particularly if you do not believe that we have properly responded to your request. The contact information, both for our Privacy Officer and the Secretary, is as follows:

Covered Entity
Attn: Privacy Officer
4600 S. Syracuse St., 11th Floor
Denver, CO 80237

Privacy Complaints
P.O. Box 8050
U.S. Dept. of Health and Human Services
Covered Entity for Medicare & Medicaid Services

7500 Security Boulevard, Baltimore, Maryland 21244-1850

_____	_____
Date	Signature of Authorized Official

ORIGINAL: To Patient (or Personal Representative)
COPY: To Patient Record Under Privacy Tab

Attachment 18
PATIENT REQUEST FOR ACCOUNTING OF PHI DISCLOSURES FORM

Name of Patient: _____

Social Security Number: _____

Date of Birth: _____

I hereby request an accurate and complete accounting of any and all Disclosures of my protected health information, or "PHI" that has been made by Covered Entity during the past six (6) years. I understand that Covered Entity is not obligated to account for any Disclosures (a) to carry out Treatment, Payment or Health Care Operations; (b) to me or my Personal Representative; (c) pursuant to an Authorization executed by me or my Personal Representative: (d) to persons involved in my care or other notification procedures; (e) for national security or intelligence purposes; (e) to correctional institutions or law enforcement officials; (f) as part of a limited data set; or (g) that occurred prior to April 14, 2003, the compliance date for the HIPAA Privacy Regulations.

_____ _____

Patient (or Personal Representative*) Signature Date

_____

Printed Name

If signed by Personal Representative, state relationship to

Patient: _____