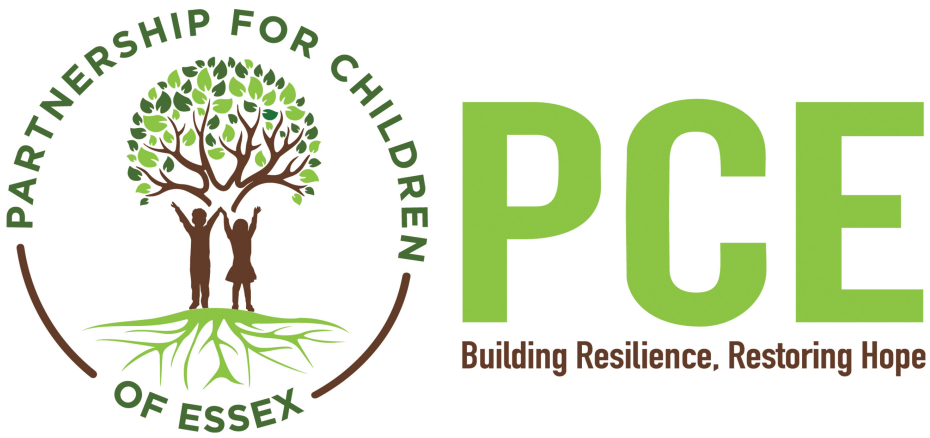

HIPAA PRIVACY RULE POLICY MANUAL

TABLE OF CONTENTS

Page

HIPAA PRIVACY POLICIES:
HIPAA COMPLIANCE PROGRAM

Topic: **HIPAA COMPLIANCE – INTRODUCTION AND ADMINISTRATIVE MATTERS**

Date Adopted: May 1, 2020

Revised:

I. INTRODUCTION

This **HIPAA Privacy Rule Policy Manual** ("Manual") contains the HIPAA Privacy Rule Policies and Procedures of **Partnership for Children of Essex** (the "**Organization**"). This Manual, together with the Organization's HIPAA Security Rule Policy Manual, comprise the Organization's HIPAA Compliance Program.

The Organization's HIPAA Compliance Program manuals outline the steps that are being taken by the Organization to comply with the Health Insurance Portability and Accountability Act of 1996, as amended including as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and their implementing regulations (collectively, "HIPAA"), and state laws and regulations governing the privacy and security of individual health information.

Reflective of the Organization's commitment to conducting business in a lawful and ethical manner, this Manual has been approved by the Organization's governing body and constitutes official Organization policy.

While the Organization recognizes that mistakes will occur, all workforce members (whether administrative, clinical or non-clinical) have an affirmative, ethical duty to come forward and report violations or suspected violations of this Manual, as well as any youth, family member/guardian or other complaint related to privacy and security, so that appropriate steps may be taken to address the issue. Workforce members who fail to comply with the policies and procedures set forth in this Manual will be subject to appropriate sanctions, including the possibility of termination. Further, compliance with these policies and procedures will be a factor in performance evaluations.

The Organization has designated a HIPAA Privacy Officer ("Privacy Officer") who oversees the implementation and oversight of the Privacy Rule Policy and Procedure Manual and privacy program for the Organization, under the guidance and oversight of the Compliance Committee.

The Organization has designated a HIPAA Security Officer ("Security Officer"), who oversees the Organization's HIPAA Security Rule Policy Manual and security program,

and who coordinates efforts with the Privacy Officer. The Security Officer operates under the guidance and oversight of the Compliance Committee.

Questions concerning the policies and procedures set forth in this Manual should be directed to the Organization's Privacy Officer. The Privacy Officer will consult with the Security Officer, Compliance Committee and/or legal counsel where appropriate.

II. PROTECTED HEALTH INFORMATION; OTHER PROTECTED INFORMATION

Throughout this Manual, references are made to "Protected Health Information" or "PHI." Under HIPAA, this term is defined to mean any health information, including genetic information, transmitted or maintained in any form, that:

- Is created or received by the Organization;
- Relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the Payment for the provision of health care to an individual; and
- Identifies the individual or offers a reasonable basis for identification.

PHI *does not include* individually identifiable health information (a) held by the Organization strictly in its role as an employer, or (b) regarding a person who has been deceased for more than 50 years.

Federal privacy requirements for covered entities, like the Organization, are contained in the HIPAA Privacy Rule and HIPAA Security Rule. These rules require the Organization to implement reasonable safeguards to protect PHI from uses and disclosures that are not permitted under HIPAA, including unauthorized access, alteration, deletion and transmission.

The HIPAA Privacy Rule governs <u>all</u> PHI, no matter what the form or format—whether oral, paper or electronic. This Manual contains the Organization's privacy policies under the Privacy Rule. In addition to HIPAA, certain New Jersey state laws impose obligations on the Organization to protect certain private information from improper uses and disclosures. These state law obligations are also addressed in this Manual.

The HIPAA Security Rule governs <u>only</u> electronic PHI, or "e-PHI," which includes PHI that is (a) transmitted by electronic means, or (b) maintained in electronic media. The Organization's policies and procedures under the Security Rule are contained in the Organization's Security Rule Policy Manual.

In addition, other federal and state laws impose obligations on the Organization to protect certain private information from improper uses and disclosures, including 42 C.F.R. Part 2 (governing the confidentiality of patient information received from federally funded substance use disorder treatment facilities) and state identity theft prevention laws.

III. TRAINING

The Organization will train all members of its workforce on the policies and procedures that comprise the Organization's HIPAA Compliance Program as necessary and appropriate for the purpose of carrying out each workforce member's job functions. New workforce members will receive training within a reasonable period of time after joining the Organization, and all workforce members will receive periodic training. In addition, if the functions of any workforce members are materially changed by amendments to the policies and procedures in this Manual, such affected workforce members will receive training in such amendments. Training will be conducted by or under the direction of the Privacy Officer.

Training will include information on at least the following topics:

- Uses and disclosures of health information
- Individual privacy rights
- Privacy breaches
- Sanctions for violations of the requirements set forth in the Organization's HIPAA Compliance Program and/or HIPAA.

Each workforce member will certify that he/she received training and understands the Organization's HIPAA Compliance Program and the requirements of HIPAA. A form for such purpose is contained in **Exhibit A**.

Each workforce member will be required to sign a Workforce Confidentiality Agreement. A form for such purpose is contained in **Exhibit B**.

IV. SANCTIONS

Any violation of the Organization's HIPAA Compliance Program by any workforce member may result in disciplinary action, up to and including termination of employment or engagement. Discipline will be dispensed promptly and consistently based upon the nature, severity, and frequency of the violation, and without regard to the seniority, rank or position of the individual in violation.

The Organization's HIPAA Sanction Policy is contained at the end of this Manual, in the policy entitled "Sanctions for Violations of HIPAA Compliance Policies and Procedures."

V. MITIGATION

The Organization will, to the extent practicable, mitigate any harmful effect due to inappropriate use or disclosure of PHI by a workforce member or by a Business Associate (or will require the Business Associate to mitigate any such harmful effect).

VI. RETALIATORY ACTS

The Organization will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the good faith exercise of any right, participation in any process, or opposition to any unlawful act or practice, set forth in the Organization's HIPAA Compliance Program. Further, the Organization will not threaten, intimidate, coerce, harass, discriminate against or take any other retaliatory action against any individual or person for:

1. Filing a complaint under 45 C.F.R. § 160.306;

2. Testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing under 45 C.F.R. Part 160;

3. Opposing any act or practice made unlawful under 45 C.F.R. Part 160, Subpart C, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of Subpart E of 45 C.F.R. Part 164.

VII. CHANGES TO POLICIES AND PROCEDURES

The Organization will promptly change the policies and procedures set forth in the Organization's HIPAA Compliance Program as necessary and appropriate to comply with changes in applicable laws or regulations. If the change materially affects the content of the Organization's Notice of Privacy Practices (the "Notice"), the Organization will promptly make appropriate revisions to the Notice in accordance with the policy contained in this Manual entitled "HIPAA Notice of Privacy Practices."

VIII. DOCUMENTATION

The Organization will maintain a written or electronic record of all written communications and any action, activity, or designation required to be documented as set forth in this Manual or related to the policies and procedures set forth herein. The Organization will retain the documentation in accordance with the applicable laws and regulations regarding the maintenance of such records, or six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

IX. REFERENCES

45 C.F.R. § 160.103 (definitions); 45 C.F.R. § 164.530(a)(1) (personnel designations); 45 C.F.R. § 164.530(b)(1) (training); 45 C.F.R. § 164.530(e)(1) (sanctions); 45 C.F.R. § 164.530(f) (mitigation); 45 C.F.R. § 164.530(g) and 45 C.F.R. § 160.316 (retaliatory acts); 45 C.F.R. § 164.530(i)(ii) (changes to policies and procedures); 45 C.F.R. § 164.530(j) (documentation).

Topic: HIPAA PRIVACY OFFICER

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization designates an individual, the HIPAA Privacy Officer ("Privacy Officer"), with responsibility for oversight of this HIPAA Privacy Rule Policy Manual and the Organization's privacy program. The Organization designates an individual, who may be the Privacy Officer or some other individual within the Organization, to serve as the HIPAA Security Officer ("Security Officer"). The Privacy Officer and Security Officer, in conjunction with the Organization's Compliance Committee, are responsible for the development, implementation, oversight and enforcement of the Organization's HIPAA Compliance Program.

II. PROCEDURES

1. The Privacy Officer is responsible for the day-to-day operation, management and enforcement of the Organization's privacy program. The Privacy Officer shall serve as a member of the Compliance Committee and shall report to the Executive Director and shall have direct access to the Organization's Board of Trustees as needed.

2. The Privacy Officer shall have authority to carry out his/her responsibilities either directly or through delegation. The Privacy Officer shall ensure supervision over delegated functions.

3. The Privacy Officer shall distribute information to workforce members regarding the Organization's HIPAA Compliance Program, along with relevant contact information. This shall include information on how to report any privacy and security compliance concerns.

4. The Privacy Officer shall possess the following minimum qualifications and experience:

   (a) Thorough knowledge and understanding of HIPAA, including the HIPAA Privacy Rule and HIPAA Security Rule, as well as state laws and regulations governing the privacy and security of health information.

   (b) Computer knowledge and skills.

(c) Experience in project management.

(d) High level of integrity and trust.

(e) Industry-related experience in HIPAA compliance or health care corporate compliance.

5. The Privacy Officer is charged with the following duties and responsibilities (i.e., job description), as may be amended from time-to-time by the Organization's governing body, in consultation with the Privacy Officer:

(a) Maintain current knowledge of applicable federal and state laws and regulations governing the privacy and security of individual health information.

(b) Oversee and monitor the development and implementation of the Organization's Privacy Rule Policy Manual, and work with the Organization's Security Officer in his/her oversight of the Organization's Security Rule Policy Manual.

(c) Coordinate activities related to HIPAA Compliance.

(d) Assist in the coordination and facilitation of allocation of appropriate resources for the support of and the effective implementation of the Organization's HIPAA Compliance Program.

(e) Act as the point of contact for (i) the reporting of privacy concerns, (ii) the receipt and management of privacy complaints, and (iii) providing further information regarding the Organization's Notice of Privacy Practices.

(f) Ensure distribution of the Organization's Privacy Rule Policy Manual and Security Rule Policy Manual to the Organization's workforce.

(g) Oversee, monitor, and ensure the delivery of initial and periodic privacy and security training and orientation to all employees, volunteers, clinical and professional staff, and other appropriate personnel, and maintain appropriate documentation of such training.

(h) Participate in determinations concerning disciplinary actions related to the failure of workforce members to comply with the Organization's HIPAA Compliance Program and/or applicable laws and regulations governing the privacy and security of individual health information.

(i) Ensure a system in in place for maintaining an inventory of all business associate contracts.

(j) Respond to and communicate with the U.S. Department of Health and Human Services, Office for Civil Rights and other governmental agencies,

with respect to any compliance reviews, audits, complaints or investigations.

(k) Work in conjunction with the Security Officer in the performance of periodic Security Rule risk and gap analyses, including through collaboration with or delegation to any business associate engaged by the Organization for such purposes.

(l) Report periodically to the Compliance Committee and Board of Trustees concerning the implementation, oversight and enforcement of the Organization's HIPAA Compliance Program.

III. REFERENCES

45 C.F.R. § 164.530

HIPAA PRIVACY POLICIES:
HIPAA COMPLIANCE PROGRAM

Topic: **HIPAA NOTICE OF PRIVACY PRACTICES**

Date Adopted: May 1, 2020

Revised:

I. POLICY

Under HIPAA, covered entities, including the Organization, are required to provide each individual receiving services from the Organization with a copy of the Organization's Notice of Privacy Practices ("Notice"). In turn, the Organization must ensure it complies with its obligations as set forth in the Notice. The Organization's Notice is included in **Exhibit C** to this Manual.

II. PROCEDURES

1. The Organization will provide a copy of the Notice to each individual receiving services from the Organization (or the parent/guardian/legal representative of an incompetent or minor) no later than the same date on which care coordination services are first provided to the individual, even if the service is provided over the telephone. The Organization must satisfy this requirement by mailing a copy of the Notice to the individual prior to service delivery, or by handing the individual the Notice when the individual comes to the Organization (or a care manager otherwise visits with the client) for services. In an emergency treatment situation, the Notice may be provided as soon as reasonably practical after the emergency has been resolved.

2. The care manager will attempt to obtain written acknowledgement from the program participant (or the parent/guardian/legal representative) that he/she has received a copy of the Notice. For this purpose, the "HIPAA Acknowledgement Form-Notice of Privacy Practices" or such other form as developed by the Organization will be used. The signed form will be scanned/placed in the individual's chart or, if the form is presented and signed in electronic format, will be maintained in electronic format in the individual's electronic health record. If written acknowledgement is not obtained, the effort of the care manager to do so must be documented in the individual's chart and a reason given for not obtaining the acknowledgement.

3. Copies of the Notice also must be available in the Organization's offices for individuals who are receiving services (or the parents/guardians) to request to take with them.

4. A copy of the Notice must be posted in a clear and prominent location within the Organization's offices (e.g., in the reception/waiting room area).

5. If the Organization maintains a website, the Organization must prominently post and make electronically available its Notice on the website.

6. The Organization may not deny medical treatment for failure to sign an acknowledgement of receipt of the Notice. The Organization may nonetheless use and disclose Protected Health Information in accordance with this Manual.

7. Whenever the Organization makes a material change to the privacy practices stated in the Notice, the Organization must (a) revise the Notice; (b) post the revised Notice in a clear and prominent location within the Organization's offices (e.g., the reception/waiting room area); (c) if the Organization maintains a website, post the revised notice on the website and make it electronically available; (d) give new program participants copies of the revised Notice and obtain written acknowledgements as described above; and (e) make the revised Notice available to existing program participants to request and take with them. The Privacy Officer shall be charged with revising the Notice and making it available for use and distribution.

III. REFERENCES

45 C.F.R. § 164.520.

HIPAA PRIVACY POLICIES:
USES AND DISCLOSURES OF PHI

Topic: **MINIMUM NECESSARY STANDARD**

Date Adopted: May 1, 2020

Revised:

I. POLICY

When using or disclosing Protected Health Information ("PHI"), or when requesting PHI from another HIPAA "covered entity," the Organization makes reasonable efforts to limit the PHI to the Limited Data Set (defined below) or, if needed, to the *minimum necessary* to accomplish the intended purpose of any use, disclosure or request.

The Organization will comply with any guidance on minimum necessary uses and disclosures that may be promulgated by the U.S. Department of Health and Human Services.

This "minimum necessary" standard will NOT apply in the following circumstances:

1. Disclosures to or requests by a health care provider for purposes of **treatment**;

2. Disclosures made **to the individual** who is the subject of the information (or to the parent/guardian/legal representative of an individual who is a minor or incompetent);

3. Disclosures made pursuant to a valid written authorization;

4. Disclosures made to the **U.S. Department of Health and Human Services** for purposes of compliance with HIPAA;

5. Disclosures that are **required by law**; and

6. Disclosures necessary for compliance with the HIPAA Privacy Rule.

II. PROCEDURES

Minimum Necessary Uses of PHI.

1. The Organization will identify which of its workforce members need access to PHI to carry out their duties, e.g., by job position or title, category or class, and which of its workforce members do not need access to PHI to carry out their duties.

2. For each job position or title, category or class of workers, the Organization will identify the category or categories of PHI to which access is needed and any conditions appropriate to such access.

3. The Organization will make reasonable efforts to limit the access of such persons or classes of such persons as determined under item 1, above, to the PHI as identified consistently with item 2, above.

Minimum Necessary Disclosures of PHI

4. For any type of disclosure the Organization makes on a routine and recurring basis, the Organization will implement policies and procedures (which may be standard protocols) that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

5. For all other disclosures, the Organization will:

   (a) Develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which the disclosure is sought; and

   (b) Review requests for disclosure on an individual basis in accordance with such criteria.

6. The Organization may rely, if such reliance is reasonable under the circumstances, on requested disclosure as the minimum necessary for the stated purpose when:

   (a) Making disclosures to public officials that are permitted under 45 C.F.R. § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose. (See the Policy below in this Manual entitled, "Other Uses and Disclosures That Do Not Require Authorization or Opportunity to Object.")

   (b) The information is being requested by another HIPAA covered entity (e.g., another health care provider or the individual's insurance company).

   (c) The information is requested by a professional who is a member of the Organization's workforce or is a business associate of the Organization for the purpose of providing professional services to the Organization, if the professional represents that the information requested is the minimum necessary for the stated purpose.

   (d) **Documentation or representations that comply with the applicable requirements of 45 C.F.R. § 164.512(i) have been provided by a person requesting the information for research purposes.*

* Italicized portion of this regulation may not be applicable to PCE.

Minimum Necessary Requests for PHI

7. The Organization will limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other HIPAA covered entities (e.g., requests made to another health care provider).

8. For a request that is made on a routine and recurring basis, the Organization must implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

9. For all other requests, the Organization must:

   (a) Develop criteria designed to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made; and

   (b) Review requests for disclosure on an individual basis in accordance with such criteria.

Other Content Requirements

10. For all uses, disclosures or requests to which the "minimum necessary" standard applies as described in this Policy, the Organization may not use, disclose or request an entire medical/health record, except when the entire medical/health record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

III. REFERENCES

45 C.F.R. § 164.502(b); 45 C.F.R. § 164.514(d).

Topic: INCIDENTAL USES AND DISCLOSURES

Date Adopted: May 1, 2020

Revised:

I. POLICY

Although it is the policy of the Organization to implement and follow reasonable safeguards regarding the use and disclosure of Protected Health Information ("PHI"), including following the "minimum necessary" standard, the Organization is cognizant that certain "incidental uses and disclosures" will occur as a result of its regular business operations. These incidental uses and disclosures are permitted, so long as the Organization uses the reasonable safeguards as set forth in this Manual.

II. PROCEDURES

1. The Organization will follow the reasonable safeguards set forth in this Manual to guard against impermissible uses and disclosures of PHI.

2. Incidental uses and disclosure of PHI are permitted. These include uses and disclosures that:

   (a) Cannot reasonably be prevented;

   (b) Are limited in nature; and

   (c) Occur as a by-product of an otherwise permitted use or disclosure.

3. Examples of incidental uses and disclosures include calling out names of program participants in the waiting room, use of sign-in sheets that list only the individual's name and non-identifying information such as time of appointment and provider/care manager being seen, and discussions in the office related to PHI where workforce members take reasonable steps to prevent such discussions from being overheard by others.

4. Workforce members will use reasonable precautions to limit incidental uses and disclosures.

III. REFERENCES

45 C.F.R. § 164.530(c)(2).

HIPAA PRIVACY POLICIES:
USES AND DISCLOSURES OF PHI

Topic: **USES AND DISCLOSURES FOR TREATMENT, PAYMENT & HEALTH CARE OPERATIONS (TPO)**

Date Adopted: May 1, 2020

Revised:

I. POLICY

As a general rule under HIPAA, subject to certain exceptions, the Organization may use or disclose an individual's Protected Health Information ("PHI") for purposes of **T**reatment, **P**ayment or Health Care **O**perations ("TPO") without obtaining the individual's consent or authorization. However, the Organization may choose to include written authorization for TPO disclosures as part of its intake forms and procedures.

However, for individuals whose records at the Organization also contain records from a substance use disorder treatment facility subject to the requirements of 42 C.F.R. Part 2 (federal regulations governing the confidentiality of individually identifiable health information received from federally funded substance use disorder treatment facilities), more stringent rules apply, as discussed below in this Policy.

II. DEFINITIONS

1. Authorization – An Authorization is a document that meets the specific requirements under HIPAA, and authorizes the use or disclosure of PHI. An Authorization must be in plain language and include the information as set forth in the Policy contained in this Manual entitled "Uses or Disclosures Requiring Written Authorization."

2. Consent – Consent is a general document that gives the Organization permission to use and disclose PHI for TPO.

3. Treatment – Treatment is defined as the provision, coordination, or management of health care and related services by one or more health care providers, including (a) the coordination or management of health care by a health care provider with a third party; (b) consultation between health care providers relating to an individual; or (c) the referral of an individual for health care from one health care provider to another.

4. Payment – Payment includes the activities undertaken by a health care provider or by a health plan to obtain or provide reimbursement for the provision of health care. Payment activities include:

(a) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(b) Billing, collection activities and related health care data processing;

(c) Review of health care services with respect to medical necessity, coverage under health plan, appropriateness of care, or justification of charges;

(d) Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and

(e) Disclosure to consumer reporting agencies of PHI relating to collection of premiums for reimbursement, of any of the following information: 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. This disclosure may be made for purposes relating to collection of reimbursement due, including the reporting not just of missed payments and overdue debt but also of subsequent positive payment experience (e.g., to expunge the debt).

5. Health Care Operations – Health Care Operations encompass the operational and administrative tasks of the Organization, including, but not limited to, the following:

(a) Quality assessment and quality improvement activities, including outcomes evaluation and development of clinical guidelines;

(b) Patient safety activities (as defined in 42 C.F.R. § 3.20);

(c) Protocol development, case management and care coordination;

(d) Contracting of health care providers and persons receiving treatment with information about Treatment alternatives;

(e) Reviewing the competence or qualifications of health care professionals;

(f) Conducting or arranging for professional services, such as legal services and auditing functions;

(g) Business planning and development; and

(h) Business management and administration.

III. PROCEDURES

1. The Organization may, but is not required to, obtain each program participant's (or the parent/guardian/legal representative of a minor or incompetent person) general written Consent for TPO disclosures during the registration process. If the Organization has in place a specific registration form containing such general consent, workforce members must make sure such form is signed during initial registration.

2. The Organization may use and disclose PHI for TPO without the individual's Consent or Authorization. TPO uses and disclosures includes the following circumstances:

   (a) For the Organization's TPO, as set forth in the Organization's Notice of Privacy Practices;

   (b) For the Treatment activities of another health care provider;

   (c) For the Payment activities of another covered entity or a health care provider, so long as the recipient is that covered entity or provider;

   (d) For another covered entity's Health Care Operations activities, so long as the recipient is that covered entity; and

   (e) For purposes of Health Care Operations between covered entities participating in a group health plan or other joint arrangement, including an organized health care arrangement.

3. *Exceptions*:

   (a) Pursuant to federal and state law, the Organization will not disclose PHI received from a federally-funded drug or alcohol treatment program, without Authorization, e.g. health records received from such a program.

   The Organization will not release psychotherapy notes for purposes of TPO except as specifically set forth in this Manual. "Psychotherapy notes" are defined under HIPAA as "notes recorded (in any medium) gy a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record." The term "psychotherapy notes" excludes 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. See the Policy in this Manual entitled "Uses and Disclosures that Require Written Authorization."

(b) The Organization will not use or disclose PHI related to HIV/AIDS without Authorization, except for Treatment purposes or as otherwise permitted by the New Jersey AIDS Assistance Act, N.J.S.A. 26:5C-1 et seq. The AIDS Assistance Act permits disclosure without Authorization under the following circumstances:

(i) To the Department of Health as required under state or federal law;

(ii) **To persons conducting research approved by an Institutional Review Board, provided that the individual's identity is not disclosed in the study or in any other manner;*

(iii) To persons conducting management or financial audits or program evaluation when such information is vital to the audit or evaluation, provided that the individual's identity is not disclosed in any report or in any other manner;

(iv) To persons directly involved in medical education or in the diagnosis and Treatment of the individual; and

(v) In all other instances authorized by state or federal law.

(c) The Organization will not use or disclose PHI for marketing purposes without Authorization, except as permitted under this Manual. See the Policy in this Manual entitled "Uses and Disclosures that Require Written Authorization."

(d) The Organization will not use or disclose PHI in a manner that constitutes a "sale" of PHI, except as permitted under this Manual. See the Policy in this Manual entitled "Uses and Disclosures that Require Written Authorization."

IV. REFERENCES

45 C.F.R. § 164.501; 45 C.F.R. § 164.506.

* Italicized portion of this regulation may not be applicable to PCE.

HIPAA PRIVACY POLICIES:
USES AND DISCLOSURES OF PHI

Topic: **OTHER USES AND DISCLOSURES THAT DO NOT REQUIRE AUTHORIZATION OR OPPORTUNITY TO OBJECT**

Date Adopted: May 1, 2020

Revised:

I. POLICY

Certain uses and disclosures of Protected Health Information ("PHI") may be made without obtaining the individual's Authorization or providing the individual with the opportunity to agree or object to the use or disclosure, as further described below in this Policy. In circumstances in which the Organization must inform the individual of, or when the individual may agree to, a use or disclosure of PHI as described below in this Policy, the Organization's information and the individual's agreement may be given orally, but should be documented in the program participant's record.

An Authorization is a document that meets the specific requirements under HIPAA, and authorizes the use or disclosure of PHI. An Authorization must be in plain language and include the information as set forth in the Policy contained in this Manual entitled "Uses or Disclosures Requiring Written Authorization."

The following uses and disclosures of Protected Health Information ("PHI") (which are explained individually in detail below) do not require an individual's Authorization:

- Uses and disclosures required by law (45 CFR 164.512(a))
- Uses and disclosures for public health activities (45 CFR 164.512(b))
- Disclosures about victims of abuse, neglect, or domestic violence (45 CFR 164.512 (c))
- Uses and disclosures for health oversight activities (45 CFR 164.512(d))
- Disclosures for judicial and administrative proceedings (45 CFR 164.512(e))
- Disclosures for law enforcement purposes (45 CFR 164.512(f))
- Uses and disclosures about decedents (45 CFR 164.512(g))
- **Uses and disclosures for cadaveric organ, eye or tissue donation (45 CFR 164.512(h))*
- *Uses and disclosures for research purposes (45 CFR 164.512(i))*
- Uses and disclosures to avert a serious threat to health or safety (45 CFR 164.512 (j))
- Uses and disclosures for specialized government functions (45 CFR 164.512(k))
- Disclosures for workers' compensation (45 CFR 164.512(l)).

* Italicized portion of this regulation may not be applicable to PCE.

II. PROCEDURE

It is advisable that workforce members consult with the Privacy Officer whenever a request for the use or disclosure of PHI is made with regard to the above situations. The Privacy Officer should consult with legal counsel when appropriate. Moreover, when such disclosures are made, members of the Organization's workforce will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting PHI.

Once it is determined that a use or disclosure of PHI is appropriate, the requested PHI will be delivered to the authorized individual or entity in a secure and confidential manner such that the information cannot be accessed by other persons who do not have appropriate authority. Workforce members shall appropriately document the request and delivery of the PHI. In the event that the identity and legal authority of an individual or entity requesting PHI cannot be verified, workforce members will refrain from disclosing the requested information and immediately contact the Privacy Officer.

1. Uses and Disclosures Required by Law.

   (a) The Organization may use or disclose an individual's PHI without the individual's Authorization if and to the extent the use or disclosure is required by federal, state or local law. By way of example, disclosure of PHI may be required (i) under state law for purposes of reporting information about victims of abuse, neglect, or domestic violence; (ii) in order to comply with court orders and subpoenas; or (iii) for law enforcement purposes. The use or disclosure must be limited to that which is necessary to comply with the law or request.

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

   (c) The Privacy Officer should be consulted prior to making any disclosure that is required by law. The Privacy Officer will consult with legal counsel when appropriate.

   (d) Refer to the policy in this Manual entitled "Responding to Subpoenas and Other Legal Requests."

2. Uses and Disclosures for Public Health Activities.

(a) The Organization may use and disclose an individual's PHI for public health activities without the individual's Authorization. By way of example, such disclosure may be made to:

(i) an authorized public health authority for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority; and may include information related to vital events such as birth or death, child abuse or neglect, or public health surveillance or investigations;

(ii) a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) a person subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity

(iv) a person who may have been exposed to a communicable disease, or who may otherwise be at risk of contracting or spreading a disease or condition, but only if authorized by law to do so. ***Note:*** this does not apply to AIDS or HIV; such information cannot be disclosed to other persons who may have been exposed without the program participant's (or parent's/guardian's/legal representative's) written authorization or court order;

(v) **an employer about an individual who is a member of the employer's workforce only in the following circumstances:*

(A) *If the Organization provides health care to the individual at the request of the employer, in order to conduct an evaluation relating to medical surveillance of the workplace, or evaluate whether the individual has a work-related illness or injury;*

(B) *If the employer needs such findings in order to comply with its obligations to record such illness or injury, or to carry out responsibilities relating to workplace medical surveillance; or*

* Italicized portion of this regulation may not be applicable to PCE.

(C) *If the Organization provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual at the time the health care is provided or by posting the notice in a prominent place at the location where the health care is provided, if the healthcare is provided on the worksite of the employer.*

*(vi) *To a school, about a student or prospective student of the school if:*

(A) The PHI that is disclosed is limited to proof of immunization;

(B) The school is required by state or other law to have such proof of immunization prior to admitting the student; and

(C) The Organization obtains and documents the agreement (which may be oral, in person or over the telephone) to the disclosure from either:

(1) A parent, guardian, or other person acting in loco parentis of the student, if the student is a minor; or

(2) The student, if the student is an adult.

3. Disclosures about Victims of Abuse, Neglect or Domestic Violence. The Organization may disclose PHI about an individual whom the Organization reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority, without the individual's Authorization.

Such a disclosure is permitted if:

(a) The disclosure is required by law and the disclosure complies with, and is limited to, the relevant requirements of such law;

(b) The individual who is the subject of the disclosure agrees to the disclosure (which agreement may be oral, but should be documented as having been obtained); or

(c) The disclosure is expressly authorized by statute or regulation, and

(i) The Organization, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(ii) If the individual is unable to agree because of incapacity, a law enforcement or other public official represents that the PHI is not

* Italicized portion of this regulation may not be applicable to PCE.

intended to be used against the individual, and that an immediate enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

The Organization will promptly inform the individual that such a report has been or will be made, EXCEPT if:

(i) The Organization believes informing the individual would place the individual at risk of serious harm; or

(ii) The Organization would be informing a personal representative, the Organization reasonably believes that the personal representative may be responsible for the abuse, neglect or other injury and informing such person would not be in the best interest of the individual.

4. Uses and Disclosures of PHI for Health Oversight Activities. The Organization may use or disclose an individual's PHI to a health oversight agency for oversight activities without the individual's Authorization. By way of example, such activities may include:

(a) Audits;

(b) Civil, administrative or criminal investigations or proceedings;

(c) Inspections;

(d) Licensure or disciplinary actions;

(e) Civil, administrative or criminal proceedings or actions; or

(f) Other activities necessary for the appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

The Organization WILL NOT release information if:

(v) The health oversight activity does not include an investigation or other activity in which the individual is the subject; and

(vi) Such investigation or other activity does not arise out of and is not directly related to:

(A) The receipt of health care,

(B) A claim for public benefits related to health, or

(C) Qualification for, or receipt of, public benefits for services.

5. Disclosures for Judicial and Administrative Proceedings. As a general rule, the Organization may, subject to the Privacy Officer's review, use or disclose PHI in the course of a judicial or administrative proceeding, without the individual's written Authorization, only in the following circumstances:

(a) In response to an order of a court or administrative tribunal, provided that the Organization discloses only the PHI expressly authorized by the order;

(b) In response to a subpoena issued by the U.S. Department of Health and Human Services, Office for Civil Rights as part of an investigation; or

(c) In response to a subpoena issued by a state licensing board (e.g., Board of Medical Examiners, Board of Dental Examiners or similar board) or state Office of the Attorney General.

Refer to the policy on "Responding to Subpoenas and Other Legal Requests," below in this Manual.

6. Disclosures for Law Enforcement Purposes. All requests for disclosures of PHI for law enforcement purposes should be referred to the Privacy Officer. The Privacy Officer will consult with legal counsel when he/she deems it appropriate.

(a) The Organization may disclose an individual's PHI to a law enforcement official for law enforcement purposes without the individual's Authorization, under any of the following conditions:

(i) Pursuant to process and as otherwise required by law – the Organization may disclose PHI:

(A) As required by law, including laws that require the reporting of certain types of wounds or other physical types of injuries.

(B) In compliance with and as limited by the relevant requirements of:

(1) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(2) A grand jury subpoena; or

(3) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that (a) the information sought is relevant and material to a legitimate law enforcement inquiry; (b) the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (c) de-identified information could not reasonably be used.

(ii) **Limited information for identification and location purposes – the Organization may disclose PHI in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, provided that the Organization will only disclose the following information for such purposes:*

(A) *Name and address;*

(B) *Date and place of birth;*

(C) *Social Security number;*

(D) *Blood type and RH factor;*

(E) *Type of injury;*

(F) *Date and time of treatment;*

(G) *Date and time of death (if applicable); and*

(H) *A description of distinguishing physical characteristics (i.e. height, weight, gender, etc.).*

The Organization WILL NOT disclose, for purposes of identification or location, any PHI related to an individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

Note: If the disclosure is required by law, the Organization must make the disclosure, including all information required to be disclosed under such law.

(iii) Victims of crime – the Organization may disclose PHI in response to a law enforcement official's request for such information about

* Italicized portion of this regulation may not be applicalbe to PCE.

an individual who is or is suspected to be a victim of a crime. However, the individual must agree to the disclosure. If the victim is unable to agree because of incapacity or other emergency circumstances, the Organization may disclose PHI if the Organization believes that it is in the best interest of the individual to do so. In addition, the law enforcement official must represent that he/she does not intend to use such information against the victim, such information is needed to determine whether a violation of the law by a person other than the victim has occurred and immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree.

Note: If the disclosure is required by law, the Organization is required to make the disclosure, including all information required to be disclosed under such law, notwithstanding the lack of Authorization from the individual.

(iv) Decedents – the Organization may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the Organization has a suspicion that such death may have resulted from criminal conduct.

(v) Crime on premises – the Organization may disclose to a law enforcement official PHI that the Organization believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the Organization.

(vi) Reporting crime in emergencies – If providing emergency health care in response to a medical emergency, other than such emergency on the premises of the Organization, the Organization may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or the victim(s) of such crime; and

(C) The identity, description and location of the perpetrator of such crime.

7. Uses and Disclosures of PHI about Decedents.

(a) The Organization may, without obtaining Authorization, disclose an individual's PHI to coroners and medical examiners for the purposes of identifying a deceased person, determining a cause of death, or other duties of coroners and medical examiners as authorized by law.

(b) The Organization may, without obtaining Authorization, disclose PHI to funeral directors, consistent with applicable state law, as necessary to carry out their duties with respect to the decedent.

(c) If the purpose of the disclosure is not as set forth above, Authorization is required and must be obtained from the executor or administrator of the estate of a deceased individual.

Note: Individually identifiable health information about an individual who has been deceased for more than 50 years is not PHI and may, therefore, be released without Authorization.

8. **Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes. The Organization may disclose an individual's PHI to entities engaged in the procurement, banking or transplantation of cadaveric organs, eye or tissue for the purpose of facilitating organ, eye, or tissue donation or transplantation without the individual's Authorization.*

9. **Uses and Disclosures of PHI for Research Purposes. The Organization may use or disclose an individual's PHI for research purposes without Authorization only in certain circumstances. Such circumstances exist when the Organization obtains documentation that an alteration to or waiver of, in whole or in part, the individual authorization otherwise required has been obtained by an Institutional Review Board (IRB) or a privacy board which meets certain requirements of the HIPAA Privacy Regulations set forth at 45 CFR 164.512(i). Such requests shall be referred to the Privacy Officer who shall consult legal counsel if necessary.*

10. Uses and Disclosures to Avert a Serious Threat to Health or Safety.

(a) The Organization may use or disclose PHI without an individual's Authorization if the Organization believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

(b) Such a disclosure may only be made to persons reasonably able to prevent or lessen the threat, including the target of the threat. If an individual admits participation in a violent crime, and the Organization reasonably believes the individual may have caused serious harm, or where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, the Organization may disclose the individual's PHI to law enforcement officials to identify or apprehend the individual. A disclosure made by an individual admitting participation in a violent crime may only contain the statement of admission and the following PHI:

(i) Name and address;

(ii) Date and place of birth;

* Italicized portion of this regulation may not be applicable to PCE.

(iii) Social security number;

(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 (i.e. height, weight, gender, race, hair and eye color, presence or absence of facial hair, beard or moustache, scars and tattoos.)

(c) The Organization may not use or disclose PHI if the information described in this section is learned in the course of treatment, counseling or therapy to affect the propensity to commit the criminal conduct, or through a request by the individual to initiate treatment, counseling or therapy.

11. Uses and Disclosures of PHI for Specialized Government Functions.

(a) The Organization may use and disclose an individual's PHI for certain specialized government functions, without the individual's Authorization. Such functions include, but are not limited to the following:

(i) Military and veterans activities;

(ii) National security and intelligence activities;

(iii) Protective services for the President and others;

(iv) Medical suitability determinations;

(v) Correctional institutions and other law enforcement custodial situations.

(b) Requests for the use and disclosure of PHI of individuals in the armed forces by military authorities or requests for the use of disclosure of PHI by authorized federal officials for the conduct of lawful intelligence, counter-intelligence and other national security activities shall be referred to the Privacy Officer who shall consult with legal counsel.

(c) The Organization may disclose PHI about an inmate or other individual to a correctional institution or law enforcement official having lawful custody of such inmate or other individual. However, the correctional institution or law enforcement official must represent that such PHI is necessary for one of the following purposes:

(i) The provision of health care to such individuals or inmate;

(ii) The health and safety of such individual or inmate;

(iii) The health and safety of the officers, workforce members or others at the correctional institution;

(iv) The health and safety of officers or other persons responsible for the transporting of inmates;

(v) Law enforcement on the premises of the correctional institution; and

(vi) The administration and maintenance of the safety, security and good order of the correctional institution.

The Organization will not consider any individual who is released on parole, probation, supervised release or otherwise is no longer in lawful custody, to be an inmate.

12. Disclosures for Workers' Compensation. The Organization may disclose PHI to the extent necessary to comply with laws relating to Workers' Compensation or other similar programs that provide benefits for work-related injuries or illness without regard to fault.

III. REFERENCES

45 CFR § 164.512(a) through (l).

HIPAA PRIVACY POLICIES:
USES AND DISCLOSURES OF PHI

Topic: RESPONDING TO SUBPOENAS AND OTHER LEGAL REQUESTS

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization will use or disclose Protected Health Information ("PHI") pursuant to a valid subpoena or other legal request only to the extent authorized by HIPAA and applicable federal and state law. The purpose of this Policy is to provide guidance in responding to subpoenas and other legal requests for records or testimony containing PHI.

II. PROCEDURES

1. Receipt of Requests. Any workforce member receiving a court order, subpoena or legal request for release of PHI (e.g., for copies of medical records or for testimony in a legal proceeding related to the contents of medical records) must immediately forward the subpoena or other request to the Privacy Officer or other individual within the Organization responsible for responding to such requests.

2. Examination of Requests. The request should be examined to determine whether the document is (a) a court order or warrant, (b) a subpoena accompanied by a court order or warrant, (c) a Grand Jury subpoena, (d) an administrative subpoena, summons or investigative demand, or (e) a subpoena that is simply an attorney request for medical records. To distinguish the difference:

   (a) Court Orders and Warrants: A court order is a legal mandate from the court and should have the following or similar phrase on the face of the document: "Order of the Court," "Order," etc., and must be signed by a judge (including an administrative law judge). A warrant operates similarly to an order, and is a document issued by a legal or government official authorizing the police or some other body to make an arrest, search premises, or carry out some other action relating to the administration of justice. Warrants must be signed by a judge or magistrate.

   (b) Subpoena Accompanied by a Court Order or Warrant: A subpoena is a summons for the recipient to produce something, and should have the word "subpoena" on the face of the document. A subpoena may be *duces tecum* (to produce documents) or *ad testificandum* (to testify orally). A

subpoena accompanied by a court order should contain the subpoena document, and be accompanied by a court order or warrant as described in (a), above.

(c) Grand Jury Subpoena: This type of subpoena will specifically contain the words "Grand Jury."

(d) Administrative Subpoena, Summons or Investigative Demand: This type of document may be issued by a governmental agency with jurisdiction over the Organization or its licensed professionals, e.g., a department of health or professional licensing board.

(e) Attorney Requested Subpoena: An attorney-requested subpoena should contain the word "subpoena" on the face of the document and will be signed by the court clerk or other officer of the court or by the requesting attorney, but is not signed ***by*** a judge.

3. Court Orders and Warrants; Subpoenas Accompanied by Court Orders or Warrants.

(a) If the request is (i) a valid court order (signed by a judge) or warrant (signed by a judge or magistrate), or (ii) a subpoena accompanied by a valid court order or warrant, the Organization must comply with the request. No information beyond that specifically requested in the document may be released.

(b) The disclosure should not be made prior to the deadline, but only on the deadline stated in the document. It is possible the Organization may receive a further notice or order attempting to "quash" or otherwise nullify the request.

(c) If the Organization receives further correspondence or documents notifying the Organization of a motion to quash or otherwise nullify the request, the Organization will await further instruction prior to releasing the requested information. If the Organization receives an order quashing or nullifying the request, or notification that the litigants have agreed to cancel the request, no documents or information may be released.

(d) Notwithstanding the above, the Organization may release PHI pursuant to a valid, HIPAA-compliant, written Authorization form signed by the individual who is the subject of the information, or his or her legally authorized representative (e.g., parent of a minor child, legal guardian or executor or administrator of the estate of a deceased individual).

Note: As a general rule, state courts or agencies issuing subpoenas or orders only have jurisdiction over entities operating within their state. Subpoenas and orders issued across state lines are generally unenforceable. Similarly, subpoenas issued by a federal court from

another state are generally unenforceable. Legal counsel should be sought in such situations. Legal counsel should be consulted for appropriate guidance.

4. Grand Jury Subpoenas. If the subpoena is issued in a Grand Jury proceeding, the Organization must strictly comply with its terms. Grand Jury proceedings are confidential, so HIPAA does not require additional protections.

5. Administrative Subpoenas, Summons, or Investigative Demands. If the Organization receives an administrative subpoena or summons, a civil or an authorized investigative demand, it may comply with the request if the issuing entity confirms: (a) the information sought is relevant and material to a legitimate law enforcement inquiry; (b) the request is specific and limited to the extent reasonably necessary for the purpose of the request; and (c) de-identified information could not reasonably be used.

6. Attorney-Requested Subpoenas. If the request is a subpoena or other attorney request that is not accompanied by a valid court order (signed by a judge) or warrant (signed by a judge or magistrate), the Organization may not release the requested information unless and until:

   (a) The Organization has received a valid, HIPAA-compliant written Authorization form signed by the individual who is the subject of the information, or his or her legally authorized representative (e.g., parent of a minor child, legal guardian or executor or administrator of the estate of a deceased individual). If a signed Authorization form was not provided with the subpoena, the Organization may either:

      (i) Contact the individual (or parent/guardian/legal representative), explaining that the Organization has received a subpoena requiring disclosure of the individual's medical record information, and notifying the individual (or parent/guardian/legal representative) that the Organization is required to respond unless the individual (or parent/guardian/legal representative) quashes or otherwise nullifies the subpoena and notifies the Organization before the deadline for responding to the subpoena. A form of notification letter is attached to the end of this Policy.

      (ii) Contact the attorney issuing the subpoena in order to request either written Authorization from the individual (or parent/guardian/legal representative) or "satisfactory assurances" from the requesting attorney before disclosure is made. Satisfactory assurances include written verification of at least one of the following:

         (A) The attorney made a good faith attempt to give the individual written notice of the subpoena, the notice included sufficient information to permit the individual to

object to the subpoena, and the time for raising objections has passed and (1) no objections were filed, or (2) all objections filed by the individual have been resolved and the disclosures being sought are consistent with such resolution; or

(B) The attorney has made reasonable efforts to secure a qualified protective order that meets the requirements of 45 C.F.R. § 164.512(e)(v). A form of attorney letter is attached to the end of this Policy.

(iii) The disclosure should not be made prior to the deadline, but only on the deadline stated in the document. (See above regarding motions to quash or nullify a subpoena.)

7. PHI Under Special Protection. Notwithstanding the above, special protections attach to certain types of PHI. The Organization will not release the following types of PHI without a valid court order (signed by a judge) or warrant (signed by a judge or magistrate) or a HIPAA-compliant written Authorization form signed by the individual who is the subject of the information, or his or her authorized legal representative (e.g., parent of a minor child, legal guardian or executor or administrator of the estate of a deceased individual):

(a) Genetic testing information (including of the individual, the individual's fetus and the individual's family members) or genetic counseling information.

(b) HIV/AIDS diagnosis or treatment information.

(c) PHI received from a federally-funded drug or alcohol treatment program.

III. REFERENCES

45 C.F.R. 164.512(e).

SAMPLE NOTIFICATION LETTER

[Next page.]

[ORGANIZATION LETTERHEAD]

[Date]

[Name]
[Address]
[Address]

Re: Subpoena for Disclosure of Health Records

Dear [Name]:

[ORGANIZATION NAME] takes health information privacy seriously and strives to maintain the privacy and confidentiality of your health record information in accordance with HIPAA and applicable state law. We are writing to advise you that we are in receipt of a subpoena seeking disclosure of your health information. A copy of the subpoena is enclosed.

The subpoena requires [ORGANIZATION NAME] to disclose the requested information by the date and time set forth in the subpoena. We may be required to provide the requested information, unless you immediately take one of the following actions:

1. Contact the attorney or other party who issued the subpoena and make arrangements to have the subpoena withdrawn or modified. Contact information is contained in the subpoena. The attorney or other party who issued the subpoena must notify our office in writing that the subpoena has been withdrawn or modified; or

2. Contact the court to obtain an order "quashing" or canceling the subpoena, or modifying it. You must provide our office with a copy of proof of such cancelation or modification.

If we do not receive the confirmation described in item (1), above, or a court order as described in item (2), above, at least 24 hours before the deadline for response as set forth in the subpoena, we may be required to disclose the information in accordance with the terms of the subpoena.

We encourage you to take prompt action regarding this letter, including contacting your legal counsel if you deem it appropriate.

Sincerely,

[name]
[title]

SAMPLE ATTORNEY LETTER

[Next page.]

[ORGANIZATION LETTERHEAD]

[Date]

[Attorney Name]
[Address]
[Address]

Re: Subpoena for Disclosure of Health Records or Information
Program Participant Name:
Case Name or Docket Number:

Dear [Attorney Name]:

[ORGANIZATION NAME] has received your subpoena for protected health information concerning the above-named individual. The Health Insurance Portability and Accountability Act of 1996 and its implementing regulations at 45 C.F.R. Parts 160 and 164 (collectively, "HIPAA") prohibit our organization from disclosing such information except in strict compliance with HIPAA.

Accordingly, as required under 45 C.F.R. § 164.512(e), you must provide one of the following to our office before we may disclose the requested protected health information:

1. A valid, written HIPAA-compliant authorization form, signed by the individual who is the subject of the protected health information, or his/her legally authorized representative (with proof of legal authority). The authorization must comply with the requirements of 45 C.F.R. § 164.508. For your convenience, I have enclosed a copy of our HIPAA-compliant authorization form.

2. A valid court order or warrant signed by a judge, magistrate or administrative tribunal with jurisdiction over [ORGANIZATION NAME], or a Grand Jury subpoena. Refer to 45 C.F.R. § 164.512(e)(1)(i) and (f)(1)(ii).

3. A valid subpoena, discovery request, or other lawful process issued from a court or administrative tribunal with jurisdiction over [ORGANIZATION NAME]. Refer to 45 C.F.R. § 164.512(e)(1)(ii). A subpoena that is not accompanied by a court order signed by a judge must be accompanied by written documentation from you confirming one of the following:

(a) That you have made a good faith attempt to provide written notice to the person who is the subject of the disclosure in enough time and with sufficient information to allow the person to object to the request, and either the person failed to timely object or the court or administrative tribunal has ruled that the information should be disclosed. Refer to 45 CFR § 164.512(e)(1)(iii); or

(b) That the parties have stipulated to or that you have obtained a protective order that prohibits the parties from using or disclosing the protected health information for any purpose

other than the pending litigation or proceeding, and requires the parties to return or destroy all copies of the protected health information at the end of the litigation or proceeding. Refer to 45 CFR § 164.512(e)(1)(iv).

Please be advised our office will disclose protected health information only upon receipt and satisfactory review of the above, and will disclose the information specifically requested only on the date required. Also note that if we have advised you of applicable copying and related fees, we must receive payment prior to the deadline for our response.

Thank you for your cooperation in assisting our organization in complying with the requirements of HIPAA.

Sincerely,

[name]
[title]

HIPAA PRIVACY POLICIES:
USES AND DISCLOSURES OF PHI

Topic: **USES AND DISCLOSURES THAT REQUIRE WRITTEN AUTHORIZATION**

Date Adopted: May 1, 2020

Revised:

I. POLICY

As described in the Policy in this Manual entitled "Uses and Disclosures for Treatment, Payment and Health Care Operations (TPO)," uses and disclosures for the Organization's TPO purposes may be made without obtaining individual Authorization. Similarly, as described in the policy in this Manual entitled "Other Uses and Disclosures that Do Not Require Authorization or an Opportunity to Object," the Organization may make certain other uses and disclosures of PHI without Authorization, as further described in that policy. All other uses and disclosures of PHI require Authorization, or require the Organization to provide the individual with an opportunity to agree or object to the use or disclosure (refer to the Policy in this Manual entitled "Uses and Disclosures that Require an Opportunity for the Individual to Agree or Object."

Under HIPAA, "Authorization" means a document authorizing disclosure of health information, written in plain language, that meets the specific requirements set forth below in this policy. Any document not meeting all requirements is not a valid Authorization.

II. PROCEDURES

1. All requests for disclosures that require an individual's Authorization will be directed to the Privacy Officer or person designated by the Privacy Officer for handling such requests. (If the request is a subpoena or court order, refer to the policy in this Manual entitled "Responding to Subpoenas and Other Legal Requests.)

2. The Organization will provide any information necessary for individuals to make an informed decision as to whether to sign an Authorization. The Organization will provide the individual with a copy of the signed Authorization.

3. The Organization will permit an individual to revoke an Authorization in writing at any time, except:

   (a) To the extent that the Organization or a business associate of the Organization has taken action in reliance on the Authorization; or

(b) The Authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy.

4. The Organization's form of HIPAA-compliant Authorization form is included in **Exhibit D** to this Manual. To the extent possible, the Organization will make efforts to have individuals sign the Organization's form of Authorization. If the Organization receives a form of Authorization from another source, the Privacy Officer or person designated by the Privacy Officer for such purposes will examine the Authorization prior to acting on it, in order to ensure it contains all required elements.

5. Elements of a Valid Authorization.

(a) An Authorization must be written in plain language and include the following information:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

(iii) The name or other specific identification of the person(s), or class of persons, to whom the Organization may make the requested use or disclosure;

(iv) A description of each purpose of the requested use or disclosure. (The statement "at the request of an individual" is a sufficient description of the purpose when an individual initiates the authorization and does not provide a statement of the purpose);

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. (The statement "end of research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research); and

(vi) Signature of the individual, date, and if the Authorization is signed by a personal representative of the individual, the name of the representative and a description of such representative's authority to act for the individual.

(b) In addition to the core elements set forth above, the Authorization must include statements adequate to place the individual on notice of the following:

(i) The individual's right to revoke the Authorization in writing, and either:

(A) the exceptions to the right to revoke and description of how the individual may revoke the Authorization; or

(B) if this information is provided in the Organization's Notice of Privacy Practices, a reference to the Notice;

(ii) The ability or inability of the Organization to condition Treatment or Payment on the receipt of an Authorization. (See "Prohibition on Conditioning of Authorizations," set forth below, to determine when conditioning is permitted); and

(iii) The potential for information to be subject to re-disclosure by recipient and to no longer be protected by the Organization.

6. Invalid Authorizations. The Organization must not honor an Authorization if:

(a) The expiration date has passed or the expiration event has occurred;

(b) The Authorization has not been filled out completely with respect to the required elements described in this policy;

(c) The Authorization has been revoked;

(d) Any material information in the Authorization is known to be false; or

(e) The Authorization violates the rules on conditioning or compound authorizations, as described below.

In such event, the Organization will contact the requesting party and advise such party that the Authorization is invalid, including the deficiencies causing the invalidity. Whenever possible, such communication should be in writing, and a copy of the invalid Authorization form and communication should be included in the program participant's chart.

7. Prohibition on Conditioning of Authorizations. The Organization may not condition the provision of treatment or payment to an individual on the provision of an Authorization, EXCEPT:

(a) *The Organization may condition the provision of research-related treatment on the provision of an Authorization for such purpose; and*

(b) The Organization may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an Authorization for the disclosure of the PHI to such third party.

8. Compound Authorizations. An Authorization cannot be combined with any other document to create a compound Authorization, unless the other document is a similar Authorization for a similar purpose (e.g., an Authorization for a use or

* Italicized portion of this regulation may not be applicable to PCE.

disclosure of psychotherapy notes may only be combined with another Authorization for a use or disclosure of psychotherapy notes).

Exception: An Authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an Authorization for the use or disclosure of PHI for a research study with another Authorization for the same research study, with an Authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where the Organization has conditioned the provision of research-related treatment on the provision of one of the Authorizations, any compound Authorization must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned Authorization.

9. **Authorization for the Use or Disclosure of Psychotherapy Notes.*

(a) *As a general rule, the Organization must obtain a separate written Authorization prior to using or disclosing psychotherapy notes.*
"Psychotherapy notes" are any notes, in any medium, recorded by a health care provider who is a mental health professional. Such notes may include documentation or analysis of the contents of a conversation during a private, group, joint, or family counseling session and that are separated from the rest of the medical record. Psychotherapy notes do not include information related to medication prescription and monitoring, counseling session times, modalities or frequency of Treatment, results of clinical tests and any summary of the following: diagnosis, Treatment plan, symptoms, prognosis, and progress to date.

(b) *The Organization may use or disclose psychotherapy notes without obtaining an individual's Authorization only for the following Treatment, Payment and Health Care Operations (TPO) purposes:*

(i) *For use by the originator of the psychotherapy notes for treatment;*

(ii) *For use or disclosure by the Organization for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;*

(iii) *For use or disclosure by the Organization to defend itself in a legal action or other proceeding brought by the individual;*

(iv) *When required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine the Organization's compliance with the HIPAA Privacy Rule;*

* Italicized portion of this regulation may not be applicable to PCE.

(v) For a use or disclosure to a health oversight agency as set forth herein;

(vi) For a use or disclosure required by law as set forth herein;

(vii) For a use or disclosure related to decedents as set forth herein;

(viii) For a use or disclosure to avert a serious threat to health or safety as set forth in herein.

10. **Authorization for the Use or Disclosure of PHI for Marketing Purposes.*

(a) *If the Organization will receive financial remuneration in connection with marketing communications, this fact must be disclosed on an Authorization to use or disclose PHI. Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.*

(b) *Marketing is defined to mean making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing does not include a communication made:*

(i) *To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the Organization in exchange for making the communication is reasonably related to the Organization's cost of making the communication.*

(ii) For the following treatment and health care operations purposes, except where the Organization receives financial remuneration in exchange for making the communication:

(A) *For treatment of an individual by the Organization, including case management or care coordination for the* individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by the Organization, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancement to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

* Italicized portion of this regulation may not be applicable to PCE.

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of "treatment."

(c) *Exceptions*: The Organization may use or disclose PHI for purposes of marketing without the individual's Authorization if the communication:

(i) Occurs in a face-to-face meeting with the individual; or

(ii) Concerns promotional gifts of nominal value.

11. **Sale of PHI.*

(a) *The Organization must obtain written Authorization from the individual for any disclosure of PHI that constitutes a "sale" of the PHI. Such Authorization must state that the disclosure will result in remuneration to the Organization.*

(b) *"Sale of PHI" means a disclosure of PHI by the Organization, or a Business Associate of the Organization on its behalf, where the Organization or the Business Associate receives direct or indirect remuneration from or on behalf of the recipient of the PHI, in exchange for the PHI.*

(c) *Exceptions. Sale of PHI does not include disclosure of PHI:*

(i) *For public health purposes as described herein;*

(ii) *For research purposes, where the only remuneration received by the Organization or its Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;*

(iii) *For treatment and payment purposes;*

(iv) *For the sale, transfer, merger, or consolidation of all or part of the Organization's business and for the due diligence related thereto;*

(v) *To or by the Organization's Business Associate for activities that the Business Associate undertakes on behalf of the Organization (or by the Business Associate to its subcontractors for activities the subcontractors take on behalf of the Business Associate);*

(vi) *To an individual who is the subject of the PHI;*

(vii) *When required by law as set forth in this Manual; and*

* Italicized portion of this regulation may not be applicable to PCE.

(viii) *For any other permitted disclosure of PHI where the only remuneration received by the Organization (or its Business Associate) is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI.*

III. REFERENCES

45 C.F.R. § 164.508.

HIPAA PRIVACY POLICIES:
USES AND DISCLOSURES OF PHI

Topic: **USES AND DISCLOSURES THAT REQUIRE AN OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR OBJECT**

Date Adopted: May 1, 2020

Revised:

I. POLICY

Certain uses and disclosures of Protected Health Information ("PHI") require that the Organization provide an opportunity for the individual who is the subject of the PHI to agree or object prior to the use or disclosure being made. The Organization may use and disclose PHI for the purposes described in this Policy, provided that the individual is informed in advance and has the opportunity to agree to, prohibit, or restrict the use or disclosure. The Organization may orally inform the individual and obtain the individual's oral agreement or objection, but should, if possible, document the discussion.

II. PROCEDURES

1. The Organization may disclose to a relative or close personal friend of the individual, or any other person identified by the individual, PHI directly relevant to such person's involvement with the individual's care or related payment. The Organization may also disclose to such persons the individual's PHI regarding the individual's location, general condition, or death.

2. If the individual is present for the use or disclosure, the Organization may only use or disclose the PHI if the Organization obtains the individual's agreement, provides the individual with an opportunity to object and the individual does not express an objection, or reasonably infers from the circumstances that the individual does not object. If the individual is not present or cannot agree or object due to incapacity or an emergency circumstance, the Organization may determine whether such a disclosure is in the best interest of the individual.

3. The Organization may also use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. The individual will be given the opportunity to object in the same manner as set forth above to the extent that doing so will not interfere with the ability to respond to emergency circumstances.

III. REFERENCES

45 C.F.R. § 164.510

HIPAA PRIVACY POLICIES:
USES AND DISCLOSURES OF PHI

Topic: **USES AND DISCLOSURES OF SENSITIVE INFORMATION**

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization implements safeguards to protect certain information it may receive which may be subject to special protections under state and federal law ("Sensitive Information"). The Organization shall use and disclose Sensitive Information only as specifically authorized by law or regulation or as authorized pursuant to the individual's valid Authorization.

An Authorization is a document that meets the specific requirements under HIPAA, and authorizes the use or disclosure of PHI. An Authorization must be in plain language and include the information as set forth in the Policy contained in this Manual entitled "Uses or Disclosures Requiring Written Authorization."

II. PROCEDURES

1. Generally – Each of the laws and regulations referenced below provides statutory and regulatory protections to information concerning the categories listed. Prior to release of information or medical records containing "Sensitive Information," the Privacy Officer will consult with the relevant law(s) to ensure compliance. As a general rule, (a) written Authorization from the individual who is the subject of the information, or (b) a court order, either of which contains specific authorization to release the "Sensitive Information," will be satisfactory. Note, however, that some laws provide for specific items to be contained within the authorization form, and that the authorization form and/or records released be accompanied by a special notice.

2. Categories of Sensitive Information.

   (a) HIV/AIDS

      (i) New Jersey AIDS Assistance Act, N.J.S.A. § 26:5C-8 et seq.

   (b) **Venereal Disease/Sexually Transmitted Diseases*

      (i) N.J.S.A. § 26:4-41.

   (c) Drug & Alcohol Treatment and Rehabilitation

* Italicized portion of this regulation may not be applicable to PCE.

(i) N.J.S.A. § 26:2B-7 et seq.

(ii) Federal Alcohol and Drug Confidentiality Rules and Regulations, 42 CFR Part 2.

(d) Mental Health Treatment and Rehabilitation

(i) N.J.S.A. § 10:37-6.79 (for state agencies or organizations under contract with state agencies)

(di) **Genetic Information*

(i) Genetic Privacy Act of New Jersey, N.J.S.A. § 10:5-43 et seq.

(ii) Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff; implementing regulations at 29 C.F.R. § 1635.1 et seq.

(dii) Minors/Emancipated Minors

(i) N.J.S.A. § 9:17B-3 (emancipated minors)

(ii) N.J.S.A. § 9:17A-1 (prenatal or relating to children of minor)

(iii) N.J.S.A. § 9:17A-4 (venereal disease, HIV/AIDS, drug/alcohol)

(iv) N.J.S.A. § 9:17A-5 (parental notification)

3. Written Authorizations.

(a) The Privacy Officer shall review each written Authorization containing a request to release any "Sensitive Information," to ensure compliance with applicable legal requirements.

(b) The Privacy Officer shall review each court order containing a request to release any "Sensitive Information," to ensure compliance with applicable legal requirements. (See the policy in this Manual on "Responding to Subpoenas and Court Orders.")

(c) Minors.

(i) In general, a parent, legal guardian or other person acting *in loco parentis* for a minor has the authority to act on behalf of such minor, including making health care related treatment decisions and giving consents, Authorizations, or approvals to treatment and uses and disclosures of the minor's health information.

(ii) However, where permitted or required by law, minors have the right to give Authorization, approval or consent to use and disclose Sensitive Information independent from such parent, guardian or

* Italicized portion of this regulation may not be applicable to PCE.

other person. Thus, generally speaking, in situations in which a minor has the legal authority to consent to medical treatment, Authorization to release protected health information must be obtained from the minor.

(iii) When responding to the request of a parent, legal guardian or other person with legal authority to inspect or obtain copies of medical records of a minor child, the Organization must ensure that when any portion of the record containing Sensitive Information of which only the minor has authority to provide Authorization:

(A) Only the authorized portion of the medical record should be viewed by or released to such individual, unless separate Authorization from the minor child is received for the portions of the medical record containing Sensitive Information of which only the minor has authority to provide Authorization; and

(B) If less than the complete medical record or portion thereof that is within the parameters of the record request is provided to the parent, legal guardian or other person with legal authority over the minor child, the records are released with the following written notice:

PLEASE BE ADVISED THAT SOME OF THE MEDICAL RECORDS OF [INSERT MINOR CHILD'S NAME] YOU HAVE REQUESTED HAVE BEEN MARKED CONFIDENTIAL AND ARE NOT AUTHORIZED FOR RELEASE WITHOUT THE WRITTEN AUTHORIZATION OF [INSERT MINOR CHILD'S NAME].

(iv) Additional information concerning consent from minors is included in **Exhibit E**.

4. Permitted Uses and Disclosures. The Organization may use and disclose Sensitive Information in its possession as authorized by the individual or otherwise permitted or authorized under applicable laws and regulations.

III. REFERENCES

N.J.S.A. § 26:5C-8 et seq.; N.J.S.A. § 26:4-41; N.J.S.A. § 26:2B-7 et seq.; 42 CFR Part 2; N.J.S.A. § 10:37-6.79; N.J.S.A. § 10:5-43 et seq.; 42 U.S.C. § 2000ff; 29 C.F.R. § 1635.1 et seq.; N.J.S.A. § 9:17B-3; N.J.S.A. § 9:17A-1; N.J.S.A. § 9:17A-4; N.J.S.A. § 9:17A-5.

HIPAA PRIVACY POLICIES:
INDIVIDUAL RIGHTS

Topic: PERSONAL REPRESENTATIVES WITH LEGAL AUTHORITY

Date Adopted: May 1, 2020

Revised:

I. POLICY

With certain exceptions, the Organization allows personal representatives who have *legal authority* (hereinafter, a "Personal Representative") in accordance with state law to act on behalf of an individual as if such Personal Representative were to have "stepped into the shoes" of the individual for purposes of access to, and use and disclosure of, the individual's Protected Health Information ("PHI"), or for requests for accountings of disclosures of PHI.

More specifically:

1. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, the Organization must treat such person as a Personal Representative, with respect to PHI relevant to such personal representation.

2. If under applicable law a parent, guardian or other person acting in *loco parentis* (in place of a parent) has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, the Organization must treat such person as a Personal Representative, with respect to PHI relevant to such personal representation. Exception: Such person may not be a Personal Representative of an unemancipated minor, and the minor has the authority on his/her own, with respect to PHI pertaining to a health care service if:

   (a) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the Personal Representative;

   (b) The minor may lawfully obtain such health care service without the consent of a parent, guardian or other person acting in loco parentis, and the minor, a court or another person authorized by law consents to such health care service; or

(c) A parent, guardian or other person acting in loco parentis assents to an agreement of confidentiality between the Organization and the minor with respect to such health care service.

3. Notwithstanding a state law or any requirement under HIPAA to the contrary, the Organization may elect not to treat a person as the Personal Representative of the individual if:

(a) The Organization has reason to believe that (i) the individual has been or may have been subjected to domestic violence, abuse or neglect by such person, or (ii) treating such person as the Personal Representative could endanger the individual; and

(b) The Organization, in the exercise of professional judgment, decides that it is not in the best interests of the individual to treat the person as the individual's Personal Representative.

4. With respect to deceased individuals, if under applicable state law an executor, administrator or other person has authority to act on behalf of a deceased individual or the individual's estate, the Organization must treat such person as the Personal Representative, with respect to PHI relevant to such personal representation.

II. PROCEDURES

1. Prior to releasing PHI to a person claiming to be a Personal Representative, the Organization will require verification of the person's authority as follows:

(a) Request identification and, where applicable, legal documentation from the person to determine whether such person has authority to act as a Personal Representative on behalf of an individual in making decisions related to health care (e.g., spouse; other next of kin; court order appointing guardian; health care power of attorney (health care proxy or advance directive naming a Personal Representative for making health care decisions); documentation proving the individual is the executor or administrator of an estate, etc.).

(b) If the documentation is sufficient to ensure that the requesting individual is an authorized Personal Representative of the individual, the Organization will treat such person as a Personal Representative, with respect to PHI relevant to the personal representation. Ensure that disclosures to a Personal Representative are in accordance with the scope of the Personal Representative's authority (e.g., limited guardian, special medical guardian).

(c) Consult other relevant policies in this Manual, including the policy entitled "Uses and Disclosures of Sensitive Information."

(d) If the documentation is not sufficient to ensure that the requesting individual is an authorized Personal Representative of the individual, the PHI may not be released to the requesting individual unless a written Authorization from the individual has been obtained. In such event, the Privacy Officer may need to be contacted for guidance.

(e) When responding to the request of a parent, legal guardian or other person with legal authority to inspect or obtain copies of medical records of a minor child, the Organization must ensure that when any portion of the record containing Sensitive Information of which only the minor has authority to provide Authorization:

(i) Only the authorized portion of the medical record should be viewed by or released to such individual, unless separate Authorization from the minor child is received for the portions of the medical record containing Sensitive Information of which only the minor has authority to provide Authorization; and

(ii) If less than the complete medical record or portion thereof that is within the parameters of the record request is provided to the parent, legal guardian or other person with legal authority over the minor child, the records are released with the following written notice:

PLEASE BE ADVISED THAT SOME OF THE MEDICAL RECORDS OF [INSERT MINOR CHILD'S NAME] YOU HAVE REQUESTED HAVE BEEN MARKED CONFIDENTIAL AND ARE NOT AUTHORIZED FOR RELEASE WITHOUT THE WRITTEN AUTHORIZATION OF [INSERT MINOR CHILD'S NAME].

III. REFERENCES

45 C.F.R. § 164.502(g).

HIPAA PRIVACY POLICIES:
INDIVIDUAL RIGHTS

Topic: CONFIDENTIAL COMMUNICATIONS FOR PHI

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization has an obligation to ensure that individuals can receive communications regarding their Protected Health Information ("PHI") in a manner and location that they feel is safe from unauthorized use or disclosure. The Organization must permit individuals to request to receive communications of PHI from the Organization by alternative means or at alternative locations. By way of example, an individual may prefer to receive mail at an address other than a home address, or may prefer to receive telephone calls at a cell phone number rather than home phone number. The Organization is required to accommodate all reasonable requests for such confidential communications.

II. PROCEDURES

1. The Organization will require an individual to make specific requests regarding confidential communications in writing, utilizing such form(s) as developed by the Organization for such purposes.

2. The Organization will not require an explanation from the individual as to the basis for the request as a condition of accommodating the request.

3. The Organization will designate an individual, who may be the Privacy Officer, to review requests for confidential communications, and to determine whether each request may be reasonably accommodated. If a specific request may not be reasonably accommodated, the Organization will contact the individual and attempt to find a mutually agreeable alternative.

4. The Organization will develop a system and processes to ensure such requests are documented in the individual's records and, when accepted by the Organization, honored for all communications of PHI with or to the individual.

5. When appropriate, the Organization may condition the provision of a reasonable accommodation on information as to how payment, if any, will be handled, and specification of an alternative address or other method of contact.

III. REFERENCES

45 C.F.R. § 164.522(b).

HIPAA PRIVACY POLICIES:
INDIVIDUAL RIGHTS

Topic: RIGHT TO INSPECT AND OBTAIN COPIES OF PHI

Date Adopted: May 1, 2020

Revised:

I. POLICY

Each individual has a general right to inspect and obtain a copy of Protected Health Information ("PHI") in a "designated record set" about that individual. However, when permitted by law, the Organization may deny an individual's request to inspect and copy PHI.

Under HIPAA, a "designated record set" is defined to mean a group of records maintained by or for the Organization that is:

1. The medical/health records and billing records about individuals maintained by or for the Organization;

2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

3. Used, in whole or in part, by or for the Organization to make decisions about individuals.

Except as specifically provided below, an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set. The exceptions are:

(a) Psychotherapy notes (defined to mean notes (in any medium) recorded by a health care provider who is a mental health professional documenting or analyzing the contents of conversations during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual's medical record; psychotherapy notes excludes 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 diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date);

(b) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(c) PHI maintained by a covered entity that is (i) subject to the Clinical Laboratory Improvement Amendments of 1988, 42 U.S.C. § 263a, to the extent the provision of access to the individual would be prohibited by law; or (ii) Exempt from CLIA, pursuant to 42 C.F.R. § 493.3(a)(2).

II. PROCEDURES

1. Individuals may request access to inspect or copies of PHI orally or in writing, but the Organization may institute a policy requiring all requests to be in writing. The form entitled "Authorization for Use and Disclosure" should be used. The form is contained in **Exhibit D**.

2. Any workforce member receiving a request should refer the request to the Privacy Officer or other individual within the Organization charged with responding to medical record requests.

3. Upon receipt of a request, and unless the request is appropriately denied, the Organization will provide an individual with the right to inspect or copy (or both) PHI in a designated record set about that individual. The Organization may either arrange with the individual a convenient time and place for the inspection of the PHI, or may send a copy of the PHI to the location requested by the individual. If an individual wishes to inspect his/her PHI at the Organization's offices, such an individual should not be left alone with any records, nor should be permitted to remove any original records from the offices.

4. If the individual requests that a person other than the individual pick up the records at the Organization's offices, the Organization will require proof of identification from the individual authorized to pick up the records. Supervision must be provided by an appropriate administrative or clinical staff member.

5. The PHI should be furnished to the individual in the form or format that the individual requests, so long as the PHI may be readily produced in that form. Individuals have the right to obtain a copy of their PHI in electronic format if the Organization uses and maintains electronic health records. Electronic records may be e-mailed or made available through a patient portal, provided that appropriate safeguards are in place, or may be made available on a portable media device given to the individual. Individuals also are permitted to designate another person or entity to be the recipient of such electronic PHI. If the individual requests PHI in a form that is not readily producible, the Organization should either provide the PHI in a legible hard copy form, or arrange with the individual for an alternative format.

6. The Organization may provide an individual with a summary of the requested PHI or an explanation of the PHI, rather than providing a copy or facilitating an inspection, but only if the individual agrees in advance to receive a summary or explanation, including the costs for producing the summary or explanation.

7. If the Organization does not maintain the requested PHI, but knows where it can be obtained, the Organization must inform the individual where to send the request.

8. In certain circumstances, persons other than the individual whose PHI is requested, are authorized to access the PHI on behalf of the individual. Generally, the situation arises in three instances: (a) minors; (b) incompetent persons; and (c) persons designated by program participants as having authorization to access their PHI.

   (a) Minors – Refer to the policy entitled "Uses and Disclosures of Sensitive Information" and the policy entitled "Personal Representatives with Legal Authority."

   (b) Incompetent Individuals – Refer to the policy entitled "Personal Representatives with Legal Authority."

   (c) Persons Designated by Competent Individuals – A competent individual may designate another individual (e.g., a family member or friend) to have access to his/her PHI. In such instances, the Organization shall make all reasonable efforts to have the individual designate such person in writing.

9. Fees for Copying PHI. The Organization may charge an individual a reasonable cost-based fee for producing a copy of PHI (or producing a summary or explanation) requested by the individual, in accordance with this Policy.

   (a) The Organization may charge an individual requesting a copy of his/her PHI in one of the following three ways:

      (i) Calculate actual labor costs to fulfill each request, as long as the labor included is only for copying (and/or creating a summary or explanation if the individual chooses to receive a summary or explanation) but not including search and retrieval time, and the labor rates used are reasonable for such activity, plus costs of any applicable supplies (paper, CD or USB drive, postage).

      (ii) In lieu of calculating labor costs individually for each request, the Organization may develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests, so long as the types of labor costs included are the ones permitted under the Privacy Rule (e.g., labor costs for copying but not for search and retrieval) and are reasonable, plus costs of any applicable supplies (paper, CD or USB drive, postage). In this case, the following guidelines should be honored:

         (A) For requests for paper copies, per page fees (calculated as described above) are acceptable.

(B) The DHHS, Office for Civil Rights does not deem per page fees to be reasonable for copies generated (whether in electronic or paper format) of PHI maintained electronically (e.g., in an EHR system).

(iii) Charge a flat fee not to exceed $6.50 (inclusive of all labor, supplies, and postage) for requests for an electronic copy of PHI maintained electronically.

(b) The $6.50 flat fee is, therefore, one option available to the Organization if it chooses not to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically. If the Organization chooses to use a flat fee or the average cost method, it may still calculate actual costs if a PHI request is considered unusual or uncommon and is not considered in its fee structure. In such a scenario, the Organization must inform the individual, as in other cases, the approximate fee in advance.

(c) The fee limitation applies whether the request is made by the individual himself/herself, or is made by the personal representative of the individual on the individual's behalf. Further, the fee limits apply when an individual (or the individual's personal representative) directs the Organization to send the PHI to a third party designated by the individual (or the individual's personal representative). This is true whether the request comes from the individual (or personal representative) or is forwarded by the third party on behalf of and at the direction of the individual (or personal representative).

(d) The fee limitations do not apply, however, when a third party directly requests PHI from the Organization and submits a written HIPAA authorization from the individual (or relies on another permission under the HIPAA Privacy Rule) for that disclosure. Where the third party is initiating a request for PHI on its own behalf, with the individual's HIPAA authorization (or pursuant to another permissible disclosure provision in the Privacy Rule), the access fee limitations do not apply. However, where the third party is forwarding, on behalf of and at the direction of the individual, the individual's access request for the Organization to direct a copy of the individual's PHI to the third party, the fee limitations do apply.

10. Timeframes for Responding to Requests.

(a) The Organization must take prompt action on an individual's request to inspect and/or copy PHI. If the request is granted, the Organization must arrange with the individual to inspect, or send a copy of, PHI within thirty (30) days of receipt of the request.

(b) If the Organization denies the request, a written denial must be sent to the individual within thirty (30) days of receipt of the request.

(c) If the PHI is needed for further treatment by another health care provider, the Organization shall take all reasonable steps necessary to provide the PHI as soon as possible.

11. Grounds for Denying Requests to Inspect and Copy PHI. In some cases, the Organization may deny an individual's request to inspect and copy PHI. The circumstances in which the Organization may deny an individual's request for PHI fall into two categories: (1) unreviewable denials; and (2) reviewable denials.

(a) Unreviewable Denials. The Organization may deny an individual's request for PHI in the following circumstances, which are not reviewable (meaning the Organization need not allow the individual the right to have the decision to deny the request reviewed by a licensed health care professional designated by the Organization to act as a reviewing official):

(i) The information requested was compiled in anticipation of, or for use in, a civil, criminal, or administrative legal proceeding;

(ii) When PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested is likely to reveal the source of the information;

(iii) **When PHI is created or maintained by the Organization in the course of research, but only for so long as the research is in progress, and only if the individual has agreed to the denial of access when consenting to participation in the research, and the Organization tells the individual that the right to inspect or copy PHI will be reinstated after the research is over;*

(iv) When the denial meets the requirements of the Privacy Act as 5 U.S.C. § 552a (only applies in limited cases when the Organization acts as a contractor to a federal agency);

(v) The information requested is psychotherapy notes;

(vi) **The information is maintained by a laboratory subject to the Clinical Laboratory Improvements Amendment of 1988 ("CLIA"), if CLIA would prohibit the laboratory from providing the information to the individual;*

(vii) *The information is maintained by a laboratory that is exempt from CLIA because it is a research laboratory that tests human specimens but does not report patient specific results for the*

* Italicized portion of this regulation may not be applicable to PCE.

diagnosis, prevention or Treatment of any disease or impairment of, or the assessment of the health of individual patients.

(b) Reviewable Denials. The Organization may also deny an individual's request for PHI in the following circumstances, provided that the individual is given a right to have such denials reviewed by a licensed health care professional designated by the Organization as a reviewing official:

(i) A licensed health care professional determines, in his/her professional judgment, that furnishing the individual with the PHI is likely to endanger the life or physical safety of the individual or of any other person;

(ii) The PHI makes reference to another person (who is not a health care provider) and a licensed health care professional determines in his/her professional judgment that furnishing the individual with the PHI may cause substantial harm to the individual or to any other person; or

(iii) The request for PHI is made by an individual's personal representative and a licensed health care professional determines, in his/her professional judgment, that furnishing the individual with the PHI is likely to cause substantial harm to the individual or to any other person.

(c) Denying Requests for Protected Health Information. If there are grounds to deny access to some of the requested PHI, but not all of it, the Organization shall provide the individual with access to any PHI for which there are no grounds for denial under this policy. All denials must be made in writing to the individual that requested the PHI. The written denial should be made timely and must state the basis for the denial. If applicable, the written denial must tell the individual about his/her review rights, as described below, and explain how to request a review. The written denial must describe how the individual can complain to the Organization and to the Secretary of the U.S. Department of Health and Human Services regarding the denial. A form for such purpose is contained in **Exhibit F**.

(d) Review of Denials for PHI. When the Organization denies a request for PHI on the basis of any reviewable grounds, the individual may request a review of the decision. The Organization shall designate an appropriate licensed health care professional to act as the reviewing official. Whenever an individual requests a review under this section, the Privacy Officer shall immediately refer the matter to the appropriate reviewing official. The reviewing official may not have participated in the original decision to deny the request for access to PHI. The reviewing official

will, within a reasonable period of time, make a final decision whether to deny or grant access. Following the reviewing official's decision, the Organization shall provide a written notice to the individual advising him or her of the final decision, and shall take such action necessary to carry out the decision.

III. REFERENCES

45 C.F.R. § 164.524.

HIPAA PRIVACY POLICIES:
INDIVIDUAL RIGHTS

Topic: REQUESTING RESTRICTIONS ON USES AND DISCLOSURES

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization will allow an individual to request that uses and disclosures of his/her PHI be restricted. The Organization will consider these requests, but is generally not required to accept them, except in the circumstance described below.

The Organization must accept a request for a restriction involving information to be sent to a health plan for payment or health care operations purposes if the disclosure relates to products or services that were paid for (by the individual or by another person on behalf of the individual, other than the health plan) solely out-of-pocket and such disclosure is not otherwise required by law.

If the Organization agrees to a requested restriction, the Organization may not make uses or disclosures that are inconsistent with such restrictions, except as provided below.

II. PROCEDURES

1. The Organization will require individuals to make requests for restrictions in writing. A request form is contained in **Exhibit G**, unless the purpose is as described in paragraph 3, below.

2. Upon receipt of a request, the Organization will determine whether it will accept the request. Such determination will be made by the Privacy Officer or other individual designated by the Organization to make such determinations. If the Organization agrees to the restriction, the Organization will not violate such restriction, unless as specified in this Manual.

3. The Organization must agree to a request for a restriction involving information to be sent to a health plan for payment or health care operations purposes if the disclosure relates to products or services that were paid for solely out-of-pocket and such disclosure is not otherwise required by law. A form for such requests is contained in **Exhibit H**.

4. If the Organization agrees to a restriction, the restriction does not apply to the following uses and disclosures:

   (a) When the use or disclosure of the restricted PHI is required by law;

(b) When the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment; provided, however, the Organization will request that such health care provider who provides emergency treatment will not further use or disclose the information;

(c) To an individual accessing his/her own PHI;

(d) To an individual requesting an accounting of his/her own PHI; or

(e) Instances for which an opportunity to agree or object is not required as explained in the policy entitled "Other Uses and Disclosures that Do Not Require an Authorization or Opportunity to Object."

5. The Organization may terminate its agreement to a restriction in the following situations:

(a) The individual agrees to or requests the termination in writing;

(b) The individual orally agrees to the termination and the oral agreement is documented; or

(c) With the exception of restrictions to health plans for services paid out-of-pocket as set forth above, the Organization informs the individual that it is terminating its agreement to a restriction. Such termination is only effective with respect to PHI created or received after it has so informed the individual.

6. The Organization will document and retain the restriction for a period of at least six (6) years from the date of its creation or the date when it last was in effect, or in accordance with applicable regulations regarding the maintenance of such records, whichever is later.

III. REFERENCES

45 C.F.R. § 164.522.

HIPAA PRIVACY POLICIES:
INDIVIDUAL RIGHTS

Topic: REQUESTS FOR AMENDMENTS TO PHI

Date Adopted: May 1, 2020

Revised:

I. POLICY

An individual has a right to request that the Organization amend Protected Health Information (PHI) about that individual. However, the Organization may deny an individual's request to amend PHI as explained below.

II. PROCEDURES

1. All requests to amend PHI in an individual's records must be made in writing and must include a reason to support the requested amendment. Individuals who make oral requests to amend PHI will be asked to make the request in writing using the form set forth on **Exhibit I**. Any workforce member who receives a written request from an individual to amend PHI shall immediately refer such request to the Privacy Officer or other person designated by the Organization to manage such requests.

2. Grounds for Denying Requests to Amend Protected Health Information. The Organization may deny an individual's request to have PHI amended if the Organization determines that the PHI:

   (a) Is accurate and complete as stated in the Organization's records;

   (b) Would not be available for inspection or copying under the policy in this Manual entitled, "Right to Inspect and Obtain Copies of PHI"; or

   (c) Was not created by the Organization; however, this ground for denial is not available if the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.

3. How to Respond to Requests to Amend PHI.

   (a) If the Organization receives a request to have PHI amended, and accepts that request, the Organization will make the amendment to the PHI.

   (b) In addition, if the Organization receives a request to have PHI amended, and accepts that request, the Organization will send a written notice to the

individual advising the individual that the amendment is accepted and requesting from the individual any relevant persons with whom the amendment must be shared. In addition, the Organization must provide the amendment to: (i) persons the individual states have received PHI and need the amendment; and (ii) persons, including the Organization's business associates, that the Organization knows have the PHI and that may have relied, or could rely, on such information to the detriment of the individual.

(c) Generally, the Organization must take action on an individual's request to have PHI amended within sixty (60) days of the Organization's receipt of the request. If the Organization, for any reason, is unable to take action on a request within the sixty (60) day timeframe, the Organization may have a single thirty (30) day extension, so long as the Organization sends, within sixty (60) days of receiving the request, a written statement to the individual stating the reasons for the delay and the date by which the Organization will complete action on the request.

4. Denying Requests to Amend PHI.

(a) If the Organization chooses to deny that request on one of the grounds listed above, then the Organization must provide the individual, in a timely manner, with a written denial that provides the following:

(i) The basis for the denial;

(ii) A description of the individual's right to submit a written statement disagreeing with the denial and telling the individual how to submit such a statement;

(iii) A statement that if the individual does not submit a statement of disagreement, the individual may request that the Organization add the individual's request for amendment, along with the statement of denial, to any future disclosure of PHI that is the subject of the amendment request; and

(iv) A statement describing how the individual may complain to the Organization and the Secretary of the U.S. Department of Health and Human Services regarding the denial.

(b) There is no appeal or review process for denials of amendment requests, but the Organization must permit the individual to submit a written statement disagreeing with all or part of the Organization's decision to deny the amendment.

(c) Whenever an individual submits such a written statement, the Organization may choose (but is not required) to prepare a written rebuttal

statement. The Organization must provide a copy of any such rebuttal to the individual who submitted the statement of disagreement.

(d) Any written statement from the individual disagreeing with the Organization's decision to deny the amendment along with any written rebuttal statement from the Organization, must be attached to the record of the PHI and forwarded to any future recipient of the PHI.

III. REFERENCES

45 C.F.R. § 164.526.

HIPAA PRIVACY POLICIES:
INDIVIDUAL RIGHTS

Topic: REQUESTS FOR ACCOUNTING OF DISCLOSURES OF PHI

Date Adopted: May 1, 2020

Revised:

I. POLICY

Individuals have a right, in certain limited circumstances, to receive from the Organization an accounting of those instances in which the Organization disclosed PHI about that individual during the six (6) year period prior to the date on which the accounting is requested. If the individual requests an accounting of disclosures for a period shorter than six (6) years, the Organization may provide a disclosure accounting covering the shorter period as requested.

Generally, the Organization need not include an accounting of the following types of disclosures:

1. Disclosures the Organization makes to carry out its treatment, payment or health care operations (TPO) (see the policy in this Manual entitled "Uses and Disclosures for Treatment, Payment and Health Care Operations");

2. Disclosures that the Organization has made to the individual who is the subject of the PHI (or to the authorized individual on his/her behalf);

3. Disclosures incident to a use or disclosure otherwise permitted by the HIPAA Privacy Rule;

4. Disclosures made pursuant to a written Authorization (see the policy in this Manual entitled "Uses and Disclosures that Require Written Authorization");

5. Disclosures to persons involved in or responsible for the individual's care in order to notify them of the individual's location, condition or death;

6. Disclosures for national security or intelligence purposes; and

7. Disclosures to correctional institutions or law enforcement officials.

II. PROCEDURES

1. All requests for an accounting of disclosures of PHI must be made in writing using the form set forth in **Exhibit J**.

2. The Organization must document or track accountings of disclosures using the form included in **Exhibit K** or other form developed by the Organization, or through its electronic medical record system.

3. An accounting of disclosures under this policy must include for each disclosure:

   (a) The date of the disclosure;

   (b) The name of the entity or persons who received the PHI about the individual;

   (c) A brief description of the PHI disclosed; and

   (d) Either (i) a brief statement of the purpose of the disclosure; or (ii) a copy of a written request for disclosure from a government agency or other entity when the disclosure is required by law.

4. If the Organization has made multiple disclosures of PHI to the same entity or person under a single request for information from a government agency, then the Organization may:

   (a) Provide all of the information required above for the first disclosure made;

   (b) Tell the individual the frequency of the disclosures made during the period requested; and

   (c) Provide the date of the last disclosure made during the period requested.

5. **If the Organization has made disclosures of PHI for a particular research purpose in accordance with § 164.412(i) of the Privacy Rule for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide the following:*

   (a) *The name of the protocol or other research activity;*

   (b) *A description of the research protocol or other research activity;*

   (c) *A description of the type of PHI disclosed;*

   (d) *The date or period during which such disclosures occurred, including the date of the last disclosure;*

   (e) *The name, address and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and*

   (f) *A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.*

* Italicized portion of this regulation may not be applicable to PCE.

6. **If it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the Organization shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.*

7. Timeliness: The Organization must take action on an individual's request for an accounting of disclosures within sixty (60) days of the Organization's receipt of the request. If the Organization, for any reason, is unable to take an action on a request within the sixty (60) day timeframe, the Organization may have a single thirty (30) day extension, so long as the Organization sends, within sixty (60) days of receiving the request, a written statement to the individual stating the reasons for the delay and the date by which the Organization will complete action on the request.

8. Fees: The Organization must provide the first accounting of disclosures in any twelve (12) month period to an individual without charge. If an individual requests more than one disclosure accounting within any twelve (12) month period, the Organization may charge the individual a cost-based fee (including labor and supply costs); however, before charging this fee the Organization must contact the individual to tell him/her about the fee in order to provide the individual with the opportunity to withdraw or modify the request.

III. REFERENCES

45 C.F.R. § 164.528.

* Italicized portion of this regulation may not be applicable to PCE.

HIPAA PRIVACY POLICIES:
INDIVIDUAL RIGHTS

Topic: PRIVACY COMPLAINTS

Date Adopted: May 1, 2020

Revised:

I. POLICY

Pursuant to HIPAA, the Organization must provide an individual with the right to complain to the Organization, as well as to the Secretary of the U.S. Department of Health and Human Services, when such individual believes the Organization may have violated his or her privacy rights or when the individual disagrees with a decision by the Organization regarding the handling of his or her Protected Health Information ("PHI").

II. PROCEDURES

1. If a program participant (or parent/guardian/legal representative on the participant's behalf) complains to any workforce member regarding the individual's privacy rights or a decision made by the Organization regarding the individual's PHI, such workforce member will refer the individual to the Privacy Officer, or will take the individual's information and provide it to the Privacy Officer for handling.

2. The Privacy Officer will request that the individual (or parent/guardian/legal representative) submit his or her complaint in writing using the form set forth on **Exhibit L**. If the individual is unwilling or unable to submit the complaint in writing, the Privacy Officer will document the complaint using the form set forth on **Exhibit L**.

3. The Privacy Officer will thoroughly investigate the complaint. Workforce members are required to assist the Privacy Officer in the investigation when so requested. If the Privacy Officer determines the complaint is unfounded, he or she will so notify the individual in writing, explaining the reason for the Privacy Officer's conclusion. The Privacy Officer may, in his or her discretion, confer with the Compliance Committee, the Organization's governing body and/or legal counsel before responding to the individual.

4. In the event the Privacy Officer concludes that there was a violation of the individual's privacy rights or that the Organization did err in the manner in which it handled the individual's PHI, the Privacy Officer will notify the Compliance Committee, the Organization's governing body and/or legal counsel for appropriate action. The action taken should include mitigating the harm caused

the individual and any action necessary to discipline the individuals involved or, in the case of the Organization's business associates, such action as required under the contract with the business associate.

(a) The Privacy Officer will document the investigation and action taken using the form set forth on **Exhibit M**.

(b) The Privacy Officer, after consulting with the Compliance Committee as needed, the Organization's governing body as needed, and/or legal counsel as needed, will inform the individual that the matter has been addressed and will provide a general summary of the action taken.

III. REFERENCES

45 C.F.R. § 164.530(a)(1).

HIPAA PRIVACY POLICIES:
BUSINESS ASSOCIATES

Topic: **BUSINESS ASSOCIATES**

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization may disclose Protected Health Information ("PHI") to a Business Associate, and may allow a Business Associate to create, receive, maintain, or transmit PHI on the Organization's behalf ***only if*** the Organization and the Business Associate enter into a written Business Associate agreement.

The term "Business Associate" means, with respect to the Organization, a person or business entity that, on behalf of the Organization (or on behalf of an organized health care arrangement in which the Organization participates), *but other than in the capacity of a member of the workforce of the Organization (or the organized health care arrangement*):

1. Creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA's Administrative Data Standards and Related Requirements subchapter, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. § 3.20, billing, benefit management, practice management, and repricing; or

2. Provides legal, actuarial, accounting, consulting, data aggregation (as defined in 45 C.F.R. § 164.501), management, administrative, accreditation, or financial services to or for the Organization (or to or for an organized health care arrangement in which the Organization participates), where the provision of services involves the disclosure of PHI from the Organization (or organized health care arrangement in which the Organization participates), or from another Business Associate of the Organization (or organized health care arrangement in which the Organization participates), to the person or business entity.

A Business Associate *includes* a subcontractor of the Business Associate that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.

A Business Associate *does not include* a health care provider, with respect to disclosures by the Organization to the health care provider concerning the treatment of the individual. (***Note, however***, that a health care provider may act as a Business Associate of the Organization if performing Business Associate functions as set forth above.)

Thus, examples of functions or activities performed by Business Associates include, but are not limited to, the following:

(a) Billing and claims processing services and administration;

(b) Data analysis, processing or administration;

(c) Utilization review/quality assurance;

(d) Patient safety activities;

(e) Benefit management;

(f) Practice management;

(g) Repricing

Business associate services include:

(a) Legal/accounting/actuarial/consulting services;

(b) Data aggregation services;

(c) Management services;

(d) Administrative services;

(e) Accreditation services;

(f) Financial services.

Business Associates are directly liable under HIPAA for impermissible uses and disclosures of PHI, for a failure to provide breach notification to the Organization, for a failure to provide access to a copy of electronic PHI to either the Organization or the individual, or the individual's designee (whichever is specified in the Business Associate agreement), for a failure to disclose PHI where required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine the Business Associate's compliance with HIPAA, for a failure to provide an accounting of disclosures, and for a failure to comply with the requirements of the HIPAA Security Rule.

II. PROCEDURES

1. The Privacy Officer, or other person designated by the Organization for such purposes, will make determinations as to functions, activities or services provided to or for the Organization that may constitute Business Associate functions, activities and services. In making these determinations, the Privacy Officer or other designated individual may consult with the Organization's governing body and/or legal counsel.

2. The Organization has developed a template Business Associate Agreement (Exhibit N) that may be used by the Organization for all arrangements with Business Associates. In the event a Business Associate refuses to sign the Business Associate Agreement template, requests modification to the template or presents the Organization with its own form of Business Associate contract, the Privacy Officer will consult with legal counsel when appropriate.

3. The Privacy Officer, or other person designated by the Organization for such purposes, will be responsible to maintain a list of all Business Associate Agreements and inventory of where such contracts are maintained.

III. REFERENCES

45 C.F.R. § 160.103; 45 C.F.R. § 164.308(b).

HIPAA PRIVACY POLICIES:
PRIVACY SAFEGUARDS

Topic: PRIVACY SAFEGUARDS

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization has implemented administrative, technical, and physical safeguards to protect the privacy of Protected Health Information ("PHI"). In addition, the Organization (1) reasonably safeguards PHI from any intentional or unintentional use or disclosure that is in violation of the Organization's HIPAA policies and procedures or applicable law; and (2) limits incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Refer to the Organization's HIPAA Security Rule Policy Manual for additional details concerning the Organization's privacy and security safeguards.

II. PROCEDURES

1. The Organization will make reasonable efforts to limit the information used or disclosed by its workforce members and agents to the minimum necessary to accomplish the intended purpose of the use, disclosure or request, unless an exception to the "minimum necessary" standard applies. See the policy in this Manual entitled "Minimum Necessary Standard."

2. The Organization will make reasonable efforts to limit incidental uses and disclosures of PHI. Workforce members will keep conversations concerning PHI to a minimum while in public places or where such conversations could be overheard by unauthorized individuals. See the policy in this Manual entitled "Incidental Uses and Disclosures."

3. PHI in any form and format must be protected and kept confidential at all times, unless use or disclosure is otherwise permitted or required under the policies and procedures contained in this Manual.

4. Privacy and Workstation Use.

   (a) The Organization will develop protocols for safekeeping PHI kept in workstations, taking into account the Organization's computer equipment and computer security options, physical layout, staffing level and program

participant population. The protocols will be based on the following principles:

(i) The Organization will implement reasonable safeguards regarding workstations where PHI is maintained to prevent unintentional disclosure to or use by anyone other than the intended user or recipient. Reasonable safeguards may include:

(A) Ensuring that workstations are not positioned in a manner that allows unauthorized persons to easily view PHI at the workstation.

(B) Setting screensavers.

(C) Restricting access to the workstations to workforce members who have a legitimate need to have such access.

(D) Ensuring that computer usernames and passwords are not shared and are reasonably protected from unauthorized access.

(E) Ensuring that documents and removable media containing PHI, including Social Security numbers, must be shredded or properly disposed of.

(ii) Paper copies of medical records or other records containing PHI shall not be accessible by unauthorized persons by leaving them in areas where they may be viewed by unauthorized persons.

(iii) The Organization may use sign-in sheets provided only the name of the individual is used and no health information is included. The time of appointment and provider being seen may be included in the sign-in sheet. Likewise, individual names may be called out in the waiting/reception rooms or other public areas provided no health information regarding the individual is announced with the name.

5. Privacy and Computer Use. The Organization will develop protocols for computer use based on the following principles:

(a) PHI may be used or disclosed only as allowed by the HIPAA Privacy Rule and/or HIPAA Security Rule, regardless of whether that use or disclosure occurs over the telephone, electronically or otherwise;

(b) Workforce members may use or disclose PHI over the computer only in a manner that reasonably safeguards the PHI from unintentional disclosure to anyone other than the intended recipient.

(c) Workforce members shall follow all policies and procedures for computer use as described in the Organization's HIPAA Security Rule Policy Manual and as directed by the Privacy Officer and Security Officer.

6. Privacy and Printer Use. The Organization will develop protocols for printer use to prevent unauthorized disclosure of PHI, based on the following principles:

(a) Ensuring that printers are not positioned or placed in areas that allow unauthorized individuals to easily access the equipment.

(b) Ensuring that procedures are put into place to prevent PHI from being left on printer trays thereby subjecting the PHI to possible disclosure, including by, for example, reminding staff members to immediately pick up print jobs and placing locked shredding containers in nearby areas.

7. Privacy and Telephone Use. The Organization will develop protocols for using or disclosing PHI over the telephone, taking into account the physical layout, staffing level and program participant population of the Organization. The protocols will be based on the following principles:

(a) Workforce members may use or disclose PHI over the telephone only in a manner that reasonably safeguards the PHI from unintentional disclosure to anyone other than the intended recipient. Reasonable safeguards may include:

(i) Ensuring that individuals in the reception area/waiting room cannot overhear telephone discussions involving PHI. If the physical layout of the offices are such that program participants and others not employed by the Organization may be able to overhear such discussions, workforce members shall take all reasonably necessary steps to handle such situations so that as little, if any, discussion involving PHI will be overheard (e.g., by speaking as quietly as reasonably possible or not speaking on a telephone where another individual is in front of or in close proximity of the person on the telephone). The use of speaker phones in open areas is expressly prohibited;

(ii) Verifying that the workforce member is speaking with the subject of the PHI or the authorized representative (by asking for individual's social security number or date of birth, etc.); and

(iii) Restricting the type and amount of information left on an individual's voicemail or answering machine.

8. Privacy and Facsimile Use. The Organization will develop protocols for using or disclosing PHI via facsimile, taking into account the physical layout, staffing level and program participant population of the Organization. The protocols will be based on the following principles:

(a) Workforce members may use or disclose PHI via facsimile only in a manner that reasonably safeguards the PHI from unintentional disclosure to anyone other than the intended recipient. Reasonable safeguards may include:

(i) Placing fax machines in areas not easily accessible to those who are not authorized to view PHI;

(ii) Utilizing a confidential fax coversheet;

(iii) Calling and/or sending a test fax to confirm the accuracy of fax numbers;

(iv) Requesting confirmation of receipt; and

(v) In the event of a misdirected fax, attempting to have the recipient return or destroy the message.

(vi) Except in the event of an emergency, workforce members will not transmit highly sensitive health information via fax, such as that pertaining to mental health, chemical dependency, sexually transmitted diseases, or HIV/AIDS. (Refer to the policy in this Manual entitled "Uses and Disclosures of Sensitive Information.")

III. REFERENCES

45 C.F.R. § 164.530(c).

HIPAA PRIVACY POLICIES:
BREACHES OF INFORMATION - HIPAA

Topic: BREACHES OF INFORMATION - HIPAA

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization will carry out its Breach (as defined below) notification obligations in compliance with HIPAA and any other federal and state notification laws and regulations. The purpose of this Policy is to provide guidelines for investigating and responding to Breaches under HIPAA. Reference should also be made to the policy in this Manual entitled, "Breaches of Information – New Jersey Identity Theft Prevention Act."

II. DEFINITIONS

"Breach" has the same meaning as set forth in 45 C.F.R. § 164.402 and means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which "compromises the security or privacy" of the PHI. The determination of whether or not the security or privacy of PHI has been compromised shall be made in accordance with the procedures set forth below.

Breach specifically excludes:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the Organization if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.
- Any inadvertent disclosure by a person who is authorized to access PHI at the Organization to another person authorized to access PHI at the Organization, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.
- A disclosure of PHI where the Organization has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

"Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary of the U.S. Department of Health & Human Services ("DHHS"). The DHHS "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or

Indecipherable to Unauthorized Individuals" may be found at the following website address:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

By way of example, encryption renders PHI unusable, unreadable or indecipherable, provided due care is given to protect any decryption keys or other passcodes that may be used to decrypt the information, that is, make it usable, readable or decipherable.

"Access" means the ability or the means necessary to read, write, modify, or communicate data/information, or otherwise use any system resource.

"Disclosure" means the release, transfer, provision of access to, or divulging in any other manner, of PHI outside the Organization.

"Use" means the sharing, employment, application, utilization, examination, or analysis of PHI within the Organization or within its authorized Business Associate.

III. PROCEDURES

1. Reporting and Initial Steps.

   (a) The Organization will implement reasonable procedures to detect any potential or actual Breach of Unsecured PHI.

   (b) Upon any workforce member's discovery or reasonable belief that a Breach has occurred, the individual will immediately contact the Privacy Officer or his/her designee to report the incident. If the suspected or alleged Breach involves electronic PHI or any electronic systems, the Security Officer will be contacted for immediate assistance.

   (c) Each workforce member will be obligated, as a condition of continued employment, to cooperate in the Organization's investigation.

   (d) The Privacy Officer will be charged with investigating, either directly or through delegation (but maintaining responsibility for supervision), the facts and circumstances concerning the potential or actual Breach. When applicable or necessary, the Security Officer will assist the Privacy Officer.

   (e) The Privacy Officer and/or Security Officer will, when necessary, assemble an incident response team to assist in incident response, investigation, mitigation and management of Breach incidents.

   (f) When necessary, the Organization will engage legal counsel and/or internal or external incident response experts to assist in the investigation and incident response.

2. Breach Discovery and Investigation.

(a) A Breach is deemed "discovered" by the Organization as of the first day on which such Breach is known to the Organization, or, by exercising reasonable diligence would have been known to the Organization.

(b) Upon notification of a potential or actual Breach, the Privacy Officer will initiate an investigation into the facts and circumstances of the incident, including the date(s), individual(s) involved, nature and extent of the impermissible disclosure, and any facts and data necessary to perform a risk assessment. If an incident response team has been assembled, and/or if the Organization has engaged legal counsel and/or internal or external incident response experts, the Privacy Officer will coordinate efforts with such individuals.

(c) The Privacy Officer will document the investigation, outcome, risk assessment and actions taken, in a confidential written report which will be retained in the Organization's records.

(d) If the suspected or actual breach involves electronic PHI, the Privacy Officer will contact the HIPAA Security Officer to assist in the investigation and incident response.

(e) When necessary due to the nature of the potential or actual Breach, the Privacy Officer or Security Officer will, directly or through delegation, take action to mitigate any further impermissible use or disclosure of PHI.

(f) Once the Privacy Officer has conducted or overseen an investigation of the incident, he/she will perform a risk assessment. Under HIPAA, any impermissible acquisition, access, use or disclosure of Unsecured PHI is *presumed* to be a Breach unless the Organization can, through a risk assessment, demonstrate that there is a low probability that the PHI has been "compromised" based upon such risk assessment. In making the risk assessment, the Privacy Officer (when appropriate, in conjunction with the Security Officer, the Organization's governing body and/or legal counsel and any internal or external incident response experts assisting the Organization) will examine and document *at least* the following factors:

(i) *The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification*.

(A) To assess this factor, consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature.

(1) For example, with respect to financial information, this includes credit card numbers, social security

numbers, or other information that increases the risk of identity theft or financial fraud.

(2) With respect to clinical information, this may involve considering not only the nature of the services or other information, but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results).

(B) In situations where there are few, if any, direct identifiers in the information impermissibly used or disclosed, determine whether the information released could be re-identified based on the context and the ability to link the information with other available information.

(ii) *The unauthorized person who used the PHI or to whom the disclosure was made.*

(A) To assess this factor, consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information.

(B) For example, if PHI is impermissibly disclosed to another entity obligated to abide by the HIPAA Privacy and Security Rules or to a Federal agency obligated to comply with the Privacy Act of 1974 and the Federal Information Security Management Act of 2002, there may be a lower probability that the PHI has been compromised because the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity.

(C) The Organization should also evaluate the likelihood of re-identification, as further discussed above.

(iii) *Whether the PHI was actually acquired or viewed.*

(A) This factor requires analysis of whether the information impermissibly used or disclosed was actually acquired or viewed, versus whether there existed only the opportunity to do so.

(B) For example, if a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the Organization could determine that the information was not actually

acquired by the unauthorized individual even though the opportunity existed.

(C) In contrast, if the Organization mailed or faxed information to the wrong individual who opened the envelope or received the fax and called the Organization to say that he/she received the information in error, then, in this case, the unauthorized recipient viewed and acquired the information.

(iv) *The extent to which the risk to the PHI has been mitigated.*

(A) The Organization should attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

(g) Results of Risk Assessment. The risk assessment and results will be documented in the confidential written report referenced above.

(i) If, after analysis of the above factors (and any other factors deemed appropriate by the Privacy Officer, Security Officer, the Organization's governing body and/or legal counsel), the Organization determines that there is a low probability that PHI has been compromised, then the impermissible acquisition, access, use or disclosure is not a Breach, and no notification to any individual, person, organization or authority is required under HIPAA. However, in such event, the Organization may choose to take action, including sanctioning the individual responsible for the issue, requiring further training, or taking other actions deemed appropriate under the circumstances. In addition, the Organization may choose to provide a written response to the individual who notified the Organization of the potential breach, providing such individual with a brief summary of the investigation and results.

(ii) If, after analysis of the above factors (and any other factors deemed appropriate by the Privacy Officer, Security Officer, the Organization's governing body and/or legal counsel), the Organization is not able to make the determination that there is a low probability that PHI has been compromised, then notification(s) must be made, as discussed below.

(h) Unsecured PHI. Notification of Breach is required when the PHI disclosed was Unsecured PHI, that is, PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary of DHHS. The DHHS "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" may be found at the following website address:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

If the PHI has been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of such technology or methodology, no notification is required.

3. Notification(s).

(a) Notification to Affected Individuals.

(i) Notification Timeline. Notice to the affected individual(s) must be made without unreasonable delay, but in no case later than sixty (60) calendar days after the Organization's discovery of the Breach of Unsecured PHI (see #2, above regarding date of discovery). Exception: If a law enforcement official informs the Organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Organization will:

(A) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting; or

(B) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement as described above is submitted during that time.

(ii) Manner of Notification.

(A) The Organization will give written notification to each affected individual by first-class mail to the individual at his or her last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(B) If the Organization knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification must be provided by first class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available. If the Organization has insufficient or out-of-date contact information for the next of kin or personal representative, the Organization is not required to provide substitute notice as set forth below.

(C) If the Organization has insufficient or out-of-date contact information for the affected individual, a substitute form of notice, as set forth below, must be provided.

(1) Where there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of notice, such as by telephone or email.

By way of example, if the Organization learns that the home address it has for one of its program participants is out-of-date but it has the individual's e-mail address, it may provide substitute notice by e-mail even if the individual has not agreed to electronic notice.

Similarly, in the same example, if the Organization has a current telephone number rather than e-mail address for the individual, then the Organization may telephone the individual and provide the information required by the notice (as set forth below) over the phone. (However, the Organization should be sensitive to not unnecessarily disclose PHI in the process of providing substitute notice, such as leaving an answering machine message that could be picked up by other household members. In such cases, the Organization should take care to limit the amount of information disclosed on an answering machine message, for example, by leaving only its name and number and indicating it has a very important message for the individual.)

(2) Alternatively, the Organization may post a notice on its website or at another location if the Organization lacks any current contact information for the individuals, so long as the posting is done in a

manner that is reasonably calculated to reach the individuals.

(D) Where there is insufficient or out-of-date contact information for 10 or more individuals, then the Organization will post a conspicuous notice for 90 days on the Organization's website that includes a toll-free number where an individual can learn whether his/her PHI was included in the Breach; or provide notice in major print or broadcast media in the geographic area where an individual can learn whether or not his/her Unsecured PHI was included in the Breach. A toll-free number must be included in the notice.

(E) If a notification requires urgency because of potential imminent misuse of Unsecured PHI, notification may be provided by telephone or other means, in addition to written notice. However, if such urgent alternate method of notice is utilized, it must be in addition to, and not in lieu of, the required direct written notice noted above.

(iii) Content of Notification. Regardless of the method by which notice is provided to affected individuals, the notification must be in plain language and must contain:

(A) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

(B) A description of the types of Unsecured PHI involved in the Breach (such as name, Social Security number, date of birth).

(C) Any steps the individual should take to protect himself or herself from potential harm resulting from the Breach of Unsecured PHI.

(D) A brief description of what the Organization is doing to investigate the Breach, to mitigate harm, and to protect against further Breaches.

(E) Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.

(b) Notice to the Media. In the event that a single Breach of Unsecured PHI event affects more than 500 residents of the same state or jurisdiction, notice will be provided to prominent media outlets serving the state and

regional area. The content of the notice to the media shall be the same as that set forth above. Notification to prominent media outlets will be made on the same date notification to affected individuals is made.

(c) Notice to the Secretary of DHHS. In the event that a single Breach of Unsecured PHI affects 500 or more individuals (regardless of the state or jurisdiction), the Organization must provide notice to the Secretary of DHHS at the same time notice is made to the affected individuals (without unreasonable delay and in no event later than 60 days from discovery of the Breach of Unsecured PHI). The Organization will notify the Secretary of DHHS in accordance with the instructions set forth at the following website address:

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

or at such website as may be provide by DHHS from time to time.

(d) Breach Log. The Organization must maintain an annual log or internal report/tracking of Breaches of Unsecured PHI involving fewer than 500 individuals per event, and must, on an annual basis, submit notification to the Secretary of DHHS of all such Breaches. Such Breaches discovered during each calendar year must be submitted no later than 60 days after the end of the calendar year. Instructions for submitting the log may be found at the website address set forth above, or at such website as may be provided by DHHS from time to time.

(e) Business Associates. Business Associates of the Organization that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose Unsecured PHI must, without unreasonable delay but within sixty (60) calendar days, notify the Organization of any Breach of Unsecured PHI known or caused by such Business Associate. The Organization will ensure that its Business Associate agreements reflect such notification requirements. Upon notification by a Business Associate of discovery of a Breach of Unsecured PHI, the Organization will be responsible to investigate the incident as described in this Policy and, where necessary, to notify affected individuals, the media and the DHHS (as described above).

(f) Sanctions and Follow-Up. The Organization will determine whether sanctions should be imposed on any workforce member(s) who may have been the cause or involved in a Breach incident. Reference should be made to the Sanction Policy in this Manual. In addition, the Organization will document and coordinate any necessary follow-up actions as a result of a Breach incident, e.g., additional workforce training, enhanced security measures, amendment of policies and procedures or other needed follow-up actions.

(g) Document Retention. The Organization will retain copies of documentation related to its Breach investigation, including, as applicable, risk assessments, Breach logs, and any notifications made pursuant to this Policy, for a period of six (6) years from the date of the document's creation or the date when it last was in effect, whichever is later.

IV. REFERENCES

45 C.F.R. Part 164, Subpart D.

HIPAA PRIVACY POLICIES:
BREACHES OF INFORMATION – NEW JERSEY IDENTITY THEFT PREVENTION ACT

Topic: **BREACHES OF INFORMATION – NEW JERSEY IDENTITY THEFT PREVENTION ACT**

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization will carry out its Breach of Security (as defined below) notification obligations in compliance with the requirements of the New Jersey Identity Theft Prevention Act, N.J.S.A. § 56:8-161 through 166 and N.J.S.A. § 56:11-44 through 52 (the "NJITPA"). The purpose of this Policy is to provide guidelines for investigating and responding to Breaches of Security, as defined in the NJITPA. Reference should also be made to the policy in this Manual entitled, "Breaches of Information – HIPAA."

The primary purpose of the New Jersey Identity Theft Prevention Act is to ensure New Jersey businesses take measures to protect sensitive information such as Social Security numbers, to prevent identity theft and to make reports of identified incidents involving New Jersey residents in order for affected individuals to take protective measures and, where appropriate, for law enforcement agencies to be contacted. As such, the Organization must ensure protective measures are put into place to keep secure all "Personal Information" of "Customers" (as such terms are defined below) it maintains and to prevent unauthorized disclosure.

In addition, the Organization will comply with the prohibitions contained in the NJITPA concerning the display of Social Security numbers.

II. DEFINITIONS

"Breach of Security" means unauthorized access to electronic files, media or data containing Personal Information that compromises the security, confidentiality or integrity of Personal Information when access to the Personal Information has not been secured by encryption or by any other method or technology that renders the Personal Information unreadable or unusable. Good faith acquisition of Personal Information by an employee or agent of the Organization for a legitimate business purpose is not a Breach of Security, provided that the Personal Information is not used for a purpose unrelated to the Organization or subject to further unauthorized disclosure.

"Customer" means an individual who provides Personal Information to the Organization. "Customer" has been interpreted by the New Jersey Office of the Attorney General,

Division of Consumer Affairs to include customers/clients, employees, principals and other individuals whose Personal Information is received and/or maintained by an organization that conducts business in the State of New Jersey.

"Personal Information" means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security Number; (2) driver's license number or state identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute Personal Information is Personal Information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

"Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted. "Records" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed.

III. PROCEDURES

1. Reporting and Initial Steps.

   (a) The Organization will implement reasonable procedures to detect any potential or actual Breach of Security.

   (b) Upon any workforce member's discovery or reasonable belief that a Breach of Security has occurred, the individual shall immediately contact the Privacy Officer or his/her designee to report the incident. When necessary, the Privacy will contact the Security Officer.

   (c) Each workforce member will be obligated, as a condition of continued employment, to cooperate in the Organization's investigation.

   (d) The Privacy Officer will be charged with investigating, either directly or through delegation (but maintaining responsibility for supervision), the facts and circumstances concerning the potential or actual Breach of Security. When applicable or necessary, the Security Officer will assist the Privacy Officer.

   (e) The Privacy Officer and/or Security Officer will, when necessary, assemble an incident response team to assist in incident response, investigation, mitigation and management of reported incidents.

   (f) When necessary, the Organization will engage legal counsel and/or internal or external incident response experts to assist in the investigation and incident response.

2. Breach Investigation and Required Notifications.

(a) Breach Investigation.

(i) Upon notification of a potential or actual Breach of Security, the Privacy Officer will initiate an investigation into the facts and circumstances of the incident, including the date(s), individual(s) involved, nature and extent of the unauthorized disclosure, and any facts and data necessary to make a determination regarding whether a Breach of Security of Personal Information has occurred. If an incident response team has been assembled, and/or if the Organization has engaged legal counsel and/or internal or external incident response experts, the Privacy Officer will coordinate efforts with such individuals.

(ii) Once the Privacy Officer has conducted or overseen the investigation of the incident, he/she will perform an assessment to determine whether or not a Breach of Security of Personal Information has occurred, by analyzing or assessing whether:

(A) The Breach or potential Breach included the first name or first initial and last name of the affected individual(s) linked with any of the following data elements that have not been secured by encryption or other method or technology that renders the Personal Information unreadable or unusable (including through access to an encryption key or other method to re-identify encrypted or otherwise unreadable or unusable information):

(1) The Social Security numbers of any affected individual;

(2) The driver's license numbers or state identification card numbers of any affected individual; or

(3) An account number or credit or debit card number in combination with any required security code, access code, password security question, or authentication device that would permit access to an affected individual's bank account, investment account or other financial account.

(4) The Breach or potential Breach included dissociated data that, if linked, would constitute Personal Information. If so, whether the means to link the dissociated data were accessed in connection with access to the dissociated data.

(5) Whether the access was authorized or unauthorized.

(6) Whether, after examining the relevant facts and information gathered, misuse of the information is not reasonably possible.

(b) Determine Class of Individuals Involved and to Whom Report Must be Made.

(i) As a business that conducts its operations in New Jersey, the Organization must disclose any Breach of Security of computerized records containing Personal Information following discovery or notification of the Breach, to any Customer who is a resident of New Jersey and whose Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person. Disclosure of the Breach of Security to a Customer is not required if the Organization establishes that misuse of the information is not reasonably possible.

(ii) If (A) the Organization has been engaged by another business or by a public entity that conducts business in New Jersey to compile or maintain computerized records that include Personal Information on the other business's or public entity's behalf, and (B) the Organization has determined that a Breach of Security has occurred involving a Customer of that business or public entity, then, in such event, the Organization will notify the affected business or public entity in writing as soon as practicable after discovery of the Breach of Security. The affected business or public entity is thereafter legally obligated to provided notice to the affected Customers whose Personal Information was, or was reasonably believed to have been, accessed by an unauthorized person.

(c) Disclosure Requirements – Timing of Notification and To Whom Notification Must be Made.

(i) To the Affected Customer: Disclosure to the Customer must be made "in the most expedient time possible and without unreasonable delay," consistent with the legitimate needs of law enforcement, as described below, or any measures necessary to determine the scope of the Breach and restore the reasonable integrity of the data system. Disclosure to the Customer is not required if the Organization establishes that misuse of the information is not reasonably possible.

(ii) To Law Enforcement: In advance of the disclosure to the Customer, disclosure must be made to the New Jersey Division of

State Police in the Department of Law and Public Safety, for investigation and handling, which may include dissemination or referral to other appropriate law enforcement entities. Notification to the affected Customer must be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. Notification to the Customer must be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies the Organization.

(iii) By a Business or Public Entity that Compiles or Maintains Computerized Records that Include Personal Information on Behalf of the Organization: If the Organization engages another business or a public entity that conducts business in New Jersey to compile or maintain computerized records that include Personal Information on the Organization's behalf, that business or public entity is obligated to notify the Organization immediately in the event it discovers a Breach of Security involving Customers of the Organization. The Organization must thereafter notify the affected Customer(s) (and law enforcement officials when required), as described above, if the Personal Information of the affected Customer(s) was, or was reasonably believed to have been, accessed by an unauthorized person.

(iv) To Consumer Reporting Agencies: In addition to the above notification requirements, in the event the Organization discovers circumstances requiring notification of more than 1,000 persons at one time, the Organization must also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the "Fair Credit Reporting Act" (15 U.S.C. § 1681a), of the timing, distribution and content of the notices. The consumer reporting agencies are:

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374-0241
800-685-1111

Experian (www.experian.com)
P.O. Box 2104
Allen, TX 75013-0949
888-397-3742

Trans Union (www.transunion.com)
P.O. Box 1000

Chester, PA 19022
800-916-8800

(d) Disclosure Requirements – Method of Notification. Notice may be provided by one of the following methods:

(i) Written notice;

(ii) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 101 of the federal "Electronic Signatures in Global and National Commerce Act" (15 U.S.C. § 7001); or

(iii) Substitute notice, if the Organization demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Organization does not have sufficient contact information. Substitute notice must consist of all of the following:

(A) Email notice when the Organization has an email address;

(B) Conspicuous posting of the notice on the Internet web page of the Organization, if the Organization maintains one; and

(C) Notification to major statewide media.

3. Documentation Retention and Destruction.

(a) The Organization must document Breach of Security discoveries, determinations and actions taken, and retain documentation for a period of five (5) years.

(b) The Organization must destroy, or arrange for the destruction of, a Customer's Records within its custody or control containing Personal Information, which is no longer to be retained by the Organization, by shredding, erasing, or otherwise modifying the Personal Information in those Records to make it unreadable, undecipherable or nonresconstructable through generally available means.

4. Prohibited Actions Relative to Display of Social Security Numbers. In addition to the identity theft detection and notification procedures, the NJITPA contains prohibitions regarding the display of Social Security numbers, summarized as follows:

(a) The Organization may not:

(i) Publicly post or publicly display an individual's Social Security number, or any four or more consecutive numbers taken from an individual's Social Security number.

(ii) Print an individual's Social Security number on any materials that are mailed to the individual, unless state or federal law requires the Social Security number to be on the document to be mailed.

(iii) Print an individual's Social Security number on any card required for the individual to access products or services provided by the Organization.

(iv) Intentionally communicate or otherwise make available to the general public an individual's Social Security number.

(v) Require an individual to transmit his/her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.

(vi) Require an individual to use his/her Social Security number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website.

(b) The Organization may use a Social Security number for internal verification and administrative purposes, so long as the use does not require the release of the Social Security number to persons not designated by the Organization to perform associated functions allowed or authorized by law.

(c) The Organization is not prohibited from the collection, use or release of Social Security numbers as required by state or federal law.

(d) Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the Social Security number. A Social Security number that is permitted to be mailed as described in this paragraph may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been open.

(e) The foregoing prohibitions do not apply to documents that are recorded or required to be open to the public under New Jersey's public records laws, New Jersey Statutes, Title 47.

IV. REFERENCES

N.J.S.A. § 56:8-161 through 166; N.J.S.A. § 56:11-44 through 52.

HIPAA PRIVACY POLICIES
SANCTIONS FOR VIOLATIONS OF HIPAA
COMPLIANCE POLICIES AND PROCEDURES

Topic: **SANCTION POLICY**

Date Adopted: May 1, 2020

Revised:

I. POLICY

The Organization has adopted this Sanction Policy to comply with the requirements of HIPAA as well as to fulfill the Organization's duty to protect the confidentiality, security, integrity, availability and accessibility of Protected Health Information (PHI) received, maintained, used and disclosed by the Organization. All workforce members are expected and required to follow and comply with the policies and procedures contained in the Organization's HIPAA Privacy Rule Policy Manual and HIPAA Security Rule Policy Manual. These Manuals together comprise the Organization's HIPAA Compliance Program. The Organization will not tolerate violations of its HIPAA Compliance Program policies and procedures, and violations will constitute grounds for disciplinary action, up to and including termination from employment or other engagement by the Organization, as well as potential civil liability and criminal prosecution.

II. PROCEDURES

1. Any workforce member who believes, in good faith, that he/she or another workforce member has violated any policy and procedure contained in the Organization's HIPAA Compliance Program Manuals, or has inadvertently or purposefully breached the confidentiality of PHI, MUST report same to the Privacy Officer. If the reporting individual is uncomfortable reporting to the Privacy Officer for any reason, or the Privacy Officer is the perpetrator of the offense, the individual must make the report directly to the Executive Director or through the Organization's Safe Hotline to report your concerns. You may anonymously call or text Safe Hotline at 1.855.662.SAFE or complete a complaint form at SafeHotline.com/SubmitReport. You must use PCE's Company ID (5681180846) when making your complaint.

2. The Organization will not take retaliatory action against any workforce member for the good-faith reporting of HIPAA violations.

3. The Privacy Officer, and where appropriate the Security Officer, will investigate each report in consultation with the Compliance Committee. Workforce members

are required to cooperate with the Privacy Officer, Security Officer and other Organization members in any investigation under this Policy.

4. The Privacy Officer, in collaboration with the Human Resources Director, will make a recommendation for action, including sanctions where appropriate, to the Executive Director, who will review the recommendations and make a determination regarding appropriate action, including sanctions where appropriate.

5. Sanctions may include, but not necessarily be limited to, any one or more of the following:

   (a) Re-training.

   (b) Verbal or written warning.

   (c) Verbal or written reprimand.

   (d) Suspension, with or without pay.

   (e) Demotion.

   (f) Removal of right to access Protected Health Information.

   (g) Removal of right to access and utilize electronic systems and devices.

   (h) Imposition of contract penalties.

   (i) Termination.

6. Whether the violation or breach was inadvertent or purposeful, and whether the offender has repeatedly violated or breached, will be taken into consideration in determining sanctions.

7. Where appropriate, and in addition to any other action or sanction, the Privacy Officer will make a report to civil and/or criminal authorities, licensing agencies, accreditation agencies and other appropriate agencies and authorities.

III. REFERENCES

45 C.F.R. § 164.308(a)(1).

Exhibit A

Acknowledgement of HIPAA Training

Date of Training: _____

Trainer Name: _____

1. I understand that **Partnership for Children of Essex** (the "Organization") has a legal and ethical responsibility to safeguard the privacy of all program participants and to protect the confidentiality of their health information.

2. I am aware that, as part of the Organization's responsibilities, the Organization provides HIPAA privacy and security training to its staff.

3. I acknowledge that I have received HIPAA privacy and security training by the Organization. I also agree to attend future HIPAA privacy and security training sessions, as and when requested by the Organization.

4. I certify that I am familiar with the Organization's policies and procedures regarding the privacy and security of health information as contained in the Organization's HIPAA Compliance Program policy and procedure manuals, and I agree to follow those policies and procedures. I acknowledge and agree that I may be subject to disciplinary action for violating such policies and procedures as determined by the Organization, up to and including termination from my position.

5. I further agree that I will report promptly any known or suspected violations of the Organization's HIPAA policies and procedures to the Organization's Privacy Officer or Security Officer.

6. I acknowledge the Confidentiality Agreement previously signed by me. I will continue to abide by the terms and conditions of the Confidentiality Agreement.

Printed Name: _____

Title/Dept.: _____

Signature: _____ Date: _____

Exhibit B

Confidentiality Agreement

I understand that **Partnership for Children of Essex** (the "Organization") requires all employees and contractors to sign a Confidentiality Agreement as a condition of employment/engagement because of the possibility of being privy to information that is confidential and proprietary to the Organization. Information that is confidential and proprietary to the Organization includes, but is not limited to, all of the Organization's business records, forms, contracts, financial and tax information and documents, business plans, intellectual property, human resources information and records, payroll information and records, computer systems and management information, vendor information, referral source information, and individual health information and program participant records (collectively, "Confidential Information"). Additionally, I understand that the Organization has a legal and ethical responsibility to safeguard program participant privacy and to protect the confidentiality of program participant health information.

In the course of my employment/engagement by the Organization, I understand that I may come into the possession of Confidential Information.

I further understand that I must sign and comply with this Confidentiality Agreement to get authorization for access to any of the Organization's Confidential Information. I agree as follows:

1. Access to and Non-Disclosure of Confidential Information. I acknowledge that I may have access to or be provided with Confidential Information in the course of my job responsibilities. I understand, acknowledge and agree that:

(a) I will access, view, use and disclose Confidential Information, and equipment and systems containing Confidential Information, only as strictly necessary to perform legitimate and authorized work functions.

(b) I will not access, view, use or disclose Confidential Information, or equipment and systems containing Confidential Information, for any reason that is not in the performance of legitimate and authorized work functions, including for reasons of curiosity or other personal reasons.

(c) I will not access, view, use or disclose any more Confidential Information than the amount that is strictly needed to perform legitimate and authorized work functions.

(d) I will not disclose Confidential Information to others who do not have a legitimate and authorized reason to have Confidential Information, including to friends, family, significant others and co-workers who do not have a legitimate and authorized reason to have such information.

(e) I will not make inquiries about, or access, view, use or disclose, Confidential Information for or on behalf of others who do not have a legitimate and authorized reason to have Confidential Information.

(f) I will not discuss Confidential Information where unauthorized persons can overhear or view the discussion (for example, in hallways, on elevators, on public transportation, at restaurants, at social events, in other public areas, on social media or social networking forums, etc.). It is not acceptable to discuss Confidential Information that contains individual health information in public areas or public media or forums even if an individual's name is not used. Such a discussion may raise doubts among those utilizing the services of the Organization and others about the Organization's respect for privacy and may result in an impermissible breach of privacy.

(g) I will not take any Confidential Information off work premises unless authorized by my supervisor. If authorized to take Confidential Information off work premises, I will take all reasonable measures to protect such information from loss or disclosure to unauthorized individuals.

2. Access to Systems. I acknowledge that, in the course of my job responsibilities, I may have access to or be provided with access to the Organization's computers and electronic systems and devices (including portable devices) (collectively, "Systems") containing Confidential Information. I understand that the Organization reserves the right to access, view and audit all of my activity on the Systems and that the Systems (including everything within the Systems) is the property of the Organization. I further agree that:

(a) I will access and use Systems only as strictly necessary to perform legitimate and authorized work functions.

(b) I will not access or use Systems for any reason that is not in the performance of legitimate and authorized work functions, including for reasons of curiosity or other personal reasons and including for personal internet research or inquiries, personal emails or social media posts, gaming, etc.

(c) I will not take any Systems off work premises or access Systems from off-site locations unless authorized by my supervisor. If authorized to take any Systems off work premises, I will take all reasonable measures to protect such Systems and information therein from loss or disclosure to unauthorized individuals, including by using secure private (non-public) networks.

(d) I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information, applications, programs, documents or other information in the Systems, with the understanding that unauthorized transmissions include, but are not necessarily limited to, removing and/or transferring Confidential Information in any Systems to unauthorized locations (e.g., home systems and personal devices).

(e) I will comply with any and all policies, procedures and protocols adopted by the Organization for use and protection of the Systems and information therein, including that:

(i) I will protect the privacy and security of all log-on information and passcodes assigned to or adopted by me for accessing and using the Systems, and will not share same with anyone other than the Organization's Security Officer or Systems administrator.

(ii) I will follow all protocols for changing of usernames and passcodes at such periodic intervals as required or requested by the Organization.

(iii) I will not use or access the log-on information or passcode of any other workforce member.

(iv) I will follow all Organization protocols for protecting the privacy and security of workstations and Systems, and will not disable, disengage, disassemble or remove any security program, application, device or equipment.

(v) I will log off any computer or workstation prior to leaving it unattended.

3. Privacy Compliance Programs; Reporting of Privacy Concerns; Disciplinary Action.

(a) I will comply with any and all policies, procedures and protocols established and adopted by the Organization relating to the privacy and security of individual health information, Confidential Information and Systems. Further, I will participate fully in any and all privacy and security educational programs as offered and/or required by the Organization during the term of my employment or contractual engagement.

(b) I will report any breach or suspected breach (whether accidental or purposeful) by me, and my knowledge of any breach or suspected breach (whether accidental or purposeful) by another workforce member, of privacy, security, confidentiality or any Organization policy, procedure or protocol, or any state or federal law or regulation, to the individuals designated by the Organization as the organization's privacy officer, security officer or compliance officer. If the Organization maintains a compliance hotline for such reporting purposes, I may make such reports using the hotline if permitted under the applicable Organization policy. I will provide full cooperation to the Organization in its investigation and response to any privacy or other compliance concern or report.

(c) I acknowledge and understand that any violation by me of this Agreement, or violation of any Organization policy, procedure, protocol or directive, or violation of any law or regulation, will subject me to potential sanctions, including the potential for suspension (with or without pay) or termination from employment or contractual engagement, and including potential civil and criminal liability. I further understand, acknowledge and agree that the Organization has the right to enforce the terms and conditions of this Agreement, including through petition for an injunction or other legal or equitable action, without the posting of any cash, bond or other security, and I hereby consents to same.

(d) I understand, acknowledge and agree that, should an occasion arise in which I am unsure of my obligations under this Agreement or under any Organization policy, procedure, protocol or program, it is my responsibility to consult with my supervisor, or with the privacy officer, security officer or compliance officer as designated by the Organization.

4. Legal Demands. In the event I receive a subpoena, court order, order of a governmental agency or other legal demand ("Legal Notice") demanding disclosure of any Confidential Information or access to any Systems, I will immediately notify the Organization, and, to the extent feasible, give to the Organization as much time as possible to contest the Legal Notice before making the disclosure. Thereafter, any disclosure pursuant to such Legal Notice shall be in strict accordance therewith. Nothing in this Agreement shall be interpreted to limit or prohibit me from testifying truthfully in any forum.

5. Return of Confidential Information and Company Property. I agree to return all company property to the Organization, including Confidential Information, Systems and other company property, (a) at any time requested or demanded by a supervisor or other superior to me, and (b) at the conclusion of my employment or contractual engagement with the Organization.

6. Continuing Obligations. I understand, acknowledge and agree that my obligations under this Agreement (a) inure to the benefit of the Organization and its successors and assigns, (b) will continue after the termination of my employment or contractual engagement with the Organization, and (c) shall be binding upon me and my heirs, executors, administrators and legal representatives.

7. Miscellaneous.

(a) At-Will Employment Unchanged. If I am employed by the Organization on an at-will basis, I understand that this Agreement does not, and shall not be construed to, change my at-will employment status with the Organization.

(b) Entire Agreement; Amendments; Waivers; Severability; Assignment. This Agreement represents the entire understanding and agreement, and supersedes any prior or contemporaneous agreement, with respect to the subject matter hereof. This Agreement may be amended, supplemented or changed, and any provision hereof or thereof can be waived, only by written instrument making specific reference to this Agreement signed by the Organization and the staff member whose name appears below. The waiver by the Organization of a breach of any provision of this Agreement shall not operate or be construed as a further or continuing waiver of such breach or as a waiver of any other or subsequent breach. No failure on the part of the Organization to exercise, and no delay in exercising, any right, power or remedy hereunder shall operate as a waiver thereof, nor shall any single or partial exercise of such right, power or remedy by such party preclude any other or further exercise thereof or the exercise of any other right, power or remedy. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the balance of this Agreement shall remain in effect. The below-named staff member may not assign this Agreement, nor any duties and obligations hereunder, to any other person or entity.

(c) Governing Law; Jurisdiction. This Agreement shall be governed by and construed in accordance with the laws of the state of New Jersey, without giving effect to principles of conflicts of law.

By signing this document, the below-named staff member acknowledges that he/she has read and fully understands the terms and conditions of this Agreement and his/her duties and obligations hereunder, and that he/she has had ample time prior to signing this Agreement to review and consider the terms and conditions of this Agreement and seek legal or other counsel of his/her choosing. The below-named staff member acknowledges, accepts and agrees to the terms and conditions of the within Agreement.

Staff Member	**Supervisor/Witness**
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title/Position: _____	Title/Position: _____
Date: _____	Date: _____

EXHIBIT C

PARTNERSHIP FOR CHILREN OF ESSEX
Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL/HEALTH INFORMATION ABOUT YOU MAY BE USED AND SHARED OR DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

SUMMARY

Partnership for Children of Essex, Inc. (PCE) has a legal duty to safeguard your Protected Health Information. In this Notice, "you" or "your" means the youth who is receiving services from PCE. For youths who are under 18 years of age, the youth's rights under this Notice may be exercised by the youth's parent(s) or legal guardian(s).

This "Notice of Privacy Practices" (Notice) describes how PCE may use and disclose your "protected health information", (including under the federal privacy law known as HIPAA.) "Protected health information" or "PHI" includes any information that relates to your past, present, or future physical or mental health, the provision of health care, or the payment for this health care, that may identify you personally, such as by name, social security number, address or other identifier.

PCE is required by law to follow the terms of this Notice and to provide a copy of this Notice to you. We will not share your PHI other than as described in this Notice unless you tell us we can in writing. We will let you know if a breach of your PHI occurs that may have compromised the privacy or security of your PHI.

USES

We reserve the right to change this Notice and our privacy practices at any time, and the changes will apply to all PHI we have about you. Whenever we make an important change to our privacy policies, we will change this Notice and post a new Notice in the public areas of our offices. A copy of the Notice is also available on our website, at https://www.pcenj.org/.

HOW WE MAY USE AND DISCLOSURE YOUR PROTECTED HEALTH INFORMATION

PCE is permitted or required by law to use or disclose your PHI without your authorization in the situations described below.

Other uses and disclosures of your PHI will require your written authorization unless stated in this Notice. You may later revoke your authorization in writing, so long as PCE has not already taken action in reliance on your authorization.

- Treatment – to provide, coordinate or manage your health care and related services. Example: Disclose PHI to a treatment facility or treatment provider relating to your care. When disclosing certain highly sensitive health information (e.g., HIV or AIDS diagnosis or records received from a federally funded substance use disorder treatment facility), we will obtain your written authorization when legally required.
- Payment - To determine coverage; billing; claim management; reviews for medical necessity; and activities needed to obtain payment for your health services. Example: Obtaining approval for a hospital admission or residential placement may require disclosure of certain PHI to a health plan.
- Health Care Operations - Functions and activities required for PCE to operate its business as a health care provider. Examples: Evaluating health care performance and quality, utilization management, and reviewing health care provider competence. PCE also may disclose your PHI to PCE's attorneys, accountants and other professionals and vendors (known as "business associates") providing services to PCE as may be needed to conduct our business operations.
- Business Associates with whom PCE contracts to perform services for PCE.
- When a disclosure is required by law, for a legal proceeding, or for law enforcement. Examples: To report incidents of known or suspected abuse or neglect to appropriate governmental agencies, in a judicial or administrative proceedings pursuant to a subpoena or court order, or in order to report a crime to law enforcement officials.
- For public health activities. Example: To report information about a death or adverse incident, or information relating to a disease, disability or injury to a public health or other authority.
- For health oversight activities. Example: To assist a government or health oversight agency with audits, or civil or criminal investigations.
- *To coroners, funeral directors or for organ donation. Examples: To assist a coroner, medical examiner, or funeral director in official duties, or to assist organ procurement organizations in organ, eye, or tissue donation. **
- *For research purposes. In some circumstances, PCE may provide PHI in order to conduct medical research. **
- To avoid harm. Example: In order to avoid a serious threat to the health or safety of you, another person, or the public, we may report information to law enforcement personnel.
- For specific government functions. Example: For national security or intelligence activities.

**Italicized portion of this regulation may not be applicable to PCE.*

- For workers' compensation purposes. Example: In order to process a workers' compensation claim or comply with workers' compensation laws.
- Appointment reminders and health related benefits or services. If you do not wish to receive these communications, please let us know.

USES AND DISCLOSURES WHERE YOU HAVE THE OPPORTUNITY TO OBJECT

- PCE may provide your PHI to a family member, friend, or other person that you indicate is involved in your care or the payment for your health care, or to others to assist in disaster or relief efforts, unless you tell us you object. If you are not able to tell us your preference (e.g., you are unconscious), we may share your PHI if we believe it is in your best interest.

USES AND DISCLOSURES WHERE YOUR WRITTEN AUTHORIZATION IS REQUIRED

We must obtain your written authorization before we disclose your PHI for the following purposes:

- M*arketing. However, we may disclose PHI in a face-to-face communication or to provide a promotional gift of nominal value, without obtaining your written authorization. **
- *Sale of your PHI, as defined under HIPAA. **
- *Most sharing of psychotherapy notes if we receive them. **
- Fundraising activities. We may contact you regarding fundraising activities, but you may opt out of such communications.

INCIDENTAL USES AND DISCLOSURES

- Incidental uses and disclosures of your PHI may occur. Example: Discussions of your PHI that non-authorized persons may overhear. We implement reasonable safeguards to avoid such incidental uses and disclosures.

YOUR HEALTH INFORMATION RIGHTS

The law provides you with these rights related to your PHI:

- Inspect and Copy PHI -You may request to review and/or receive a paper or electronic copy of your PHI maintained by PCE in your "designated record set." This includes medical records; billing records; enrollment, payment, claims adjudication, and appeal records; electronic health records; and any other information used to make decisions about your health care. We will provide a copy or summary of your PHI, usually within 30 days. We may charge a reasonable, cost-based fee.
- Correct or Update PHI- If you believe that PCE has PHI about you that is incomplete or incorrect, you may request that it be amended. If PCE disagrees with your request, you will be notified in writing of the reason for the denial., which can sometimes be appealed.
- Alternative Means of Communication- If you want to receive communications from PCE in a different manner or at a different location, you may notify PCE of this. We will accommodate reasonable requests.
- Ask Us to Limit What We Share - You can ask us not to use or disclose certain of your PHI for treatment, payment, or our health care operations. We are not required to honor your request, and we may say "no" if it would affect your care. The only exception to this is if you pay for any item or service in full out-of-pocket and ask us not to share your PHI with your insurance company, we will honor your request unless a law requires otherwise.
- List of Disclosures - You may ask us for a list (accounting) of PCE's disclosures of PHI for the prior 6-year period that are not for treatment, payment, or health care operations or are not specifically authorized by you. We will provide one accounting per 12 month-period and may charge a reasonable, cost-based fee for additional accountings. We will respond to you within 60 days of receipt of your request.
- Choose Someone to Act for You - If someone has legal authority to act for you (e.g., parent of minor child, legal guardian, or health care power of attorney), that person may exercise your rights and make choices about your PHI.
- Copy of This Notice - A paper copy of this Notice will be provided to you upon registration with PCE. You may request a paper or electronic (including through email) copy from us at any time.
- Contact Information and Complaints - You may contact PCE if you have any questions about this Notice or complain if you believe PCE has violated your privacy rights by these methods: Mail: 300 Broadacres Drive, 3rd Floor, Bloomfield, NJ 07003, Attn: Compliance Manager; Phone: 973.323.3000; Email: Compliance_Manager@pcenj.org.

  You may file a written complaint with the U.S. Department of Health and Human Services by these methods: Mail: 200 Independence Avenue, S.W., Room 509F, HHH Bldg., Washington, DC 20201; Phone: 877-696-6775; Online: www.hhs.gov/ocr/privacy/hipaa/complaints/.

  PCE will not retaliate or penalize you for complaining or asserting your privacy rights in good faith.

**Italicized portion of this regulation may not be applicable to PCE.*

Acknowledgement of Receipt of:

- **Client Rights & Responsibilities**
- **Notice of Privacy Practices**
- **Risks Associated with Electronic Communication**
- **Policy on Recording Communications**

Youth's Name: _____

I have received copies of the "Client Rights & Responsibilities", "Notice of Privacy Practices", "Risks Associated with Electronic Communication" and "Policy on Recording Communications" from the Partnership for Children of Essex on_____
(Date)

I understand the content of the documents and have had any questions about these documents answered.

_____ _____
Youth Signature Date

_____ _____
Caregiver/Guardian/Parent Signature Date

_____
Printed name of Caregiver/Guardian/Parent

_____ _____
Witness Signature Date

_____
Printed name of Witness

Office Use Only

INABILITY TO OBTAIN ACKNOWLEDGEMENT RECEIPT OF NOTICE OF PRIVACY PRACTICES, CLIENT RIGHTS & RESPONSIBILITIES, AND RISKS ASSOCIATED WITH ELECTRONIC COMMUNICATION, AND POLICY ON RECORDING COMMUNICATIONS.
To be completed only if no signature is obtained. If it is not possible to obtain the individual's acknowledgement, describe the good faith efforts made to obtain the individual's acknowledgement, and the reason the acknowledgement was not obtained.

Reason: _____

_____ _____
Signature of Staff Member Date

_____
Printed Name

Revised 8/19/2020

EXHIBIT D

Authorization to Release Medical Information

Attached.

AUTHORIZATION TO RELEASE AND DISCLOSE HEALTH INFORMATION

Demographic Information	Name of Youth:_____ Date of Birth: _____ Address:_____ Day Phone: _____ City:_____ State:_____ Zip:_____
Receiving Party (*Where do you want the information sent? Who may have the information?*)	Name:_____ Phone: _____ Address:_____ City:_____ State:_____ Zip: _____
Information to be Released (*What do you want to be sent or released? Check the appropriate box(es).*)	☐ **Complete record** (includes ALL record types below) OR only: ☐ All ISPs (service plans and authorizations) ☐ Signed releases and other signed paperwork ☐ All formal correspondence (no-contact letters, court letters, SRTU letters, etc.) ☐ Attendance forms ☐ Strength and Needs Assessments ☐ Progress notes authored by PCENJ staff ☐ Service plans authored by PCENJ staff *Optional:* Include only the following dates of service: _____
Purpose for Release (*Why is it needed?*)	☐ Continuing care ☐ School ☐ Research ☐ Legal ☐ Insurance ☐ Other: _____

- This authorization lasts for one year after the date you sign it unless you enter a different date here: _____
- PCENJ may take up to two weeks to process this request.
- This authorization may be canceled in writing at any time by providing written notice to PCENJ, Attn: Privacy Officer. A cancellation will not change releases that happened before the cancellation.
- PCENJ will not restrict my/my youth's treatment if I choose not to sign this authorization.
- A photocopy or other electronic copy of this authorization will be treated as an original.
- PCENJ cannot provide records that we did not create, however additional records created by other professionals and organizations may be available to you. Contact your care manager for details on how to access them.
- PCENJ cannot prevent re-disclosure of your information by the person or organization that receives your records under this authorization, and that information may not be covered by state and federal privacy protections after it is released. By signing this authorization, you release PCENJ from any and all liability resulting from disclosure by the recipient.

Your signature below indicates you have read and understand this form and authorize the release of your/your youth's information as described above.

_____ _____

Signature of Individual or Legal Guardian/Legal Representative Date

_____ _____

Print name of Individual or Legal Guardian/Legal Representative Relationship to Individual

Phone: 973-323-3000 Fax: 973-323-3015
300 Broadacres Dr. 3rd Fl. Bloomfield, NJ 07003

EXHIBIT E
Consent From Minors

Note: For confidentiality issues relating to minors, please refer to the policy in this Manual entitled "Uses and Disclosures of Sensitive Information."

- Under New Jersey law, minors are defined as persons under the age of 18 years. (Reference: N.J.S.A. §§ 9:17B-1 and B-3.)

- New Jersey is not an "emancipation" state; as such, there is no specific statutory or regulatory provision granting emancipation status under given circumstances for informed consent purposes. However, a minor who has been declared by a court or an administrative agency to be emancipated may consent to any health treatment for the emancipated minor without authorization or consent from the minor's parent or legal guardian. In such circumstances, it is best to seek and review a copy of the court order granting emancipation status. A minor who is married, has entered military service, or has a child or is pregnant, may be considered emancipated for informed consent purposes. (Reference: E.g., N.J.S.A. § 2C:25-19 (emancipation status as related to domestic violence); N.J.S.A. § 55:15L-2 (emancipation status as related to public housing); N.J.S.A. § 9:17A-1.)

- A minor who is married, is pregnant, has a child or has entered military service may consent to any health treatment related to the minor without authorization from the minor's parent or legal guardian. A minor parent may also consent to all medical care for the minor's child(ren). (Reference: N.J.S.A. § 9:17A-1.)

- A minor may obtain prescription contraceptives without authorization or consent of a parent or legal guardian only if the minor is married, is pregnant, has a child, or has entered military service. In such circumstances, consent may be obtained from the minor. (Reference: N.J.S.A. § 9:17A-1.) Under federal law, a minor may obtain emergency contraceptives such as the "Plan B Morning After Pill" without authorization or consent of a parent or guardian, and without a prescription.
    - Note: Federal law prohibits the imposition of parental consent requirements on minors who obtain contraceptives/family planning services at facilities receiving funding through Title X of the Public Health Services Act, 42 U.S.C. § 300, et.seq., or Medicaid, 42 U.S.C. § 1396a(10)(A). Thus, any minor may receive these services at such sites without parental or guardian consent.

- A minor in New Jersey may obtain an abortion without mandated parental consent or notification. New Jersey law does not require the release of medical records pertaining to a minor's abortion to her parents or guardian. (Reference: N.J.S.A. § 9:17A-1.)
    - Note: The New Jersey *Parental Notification for Abortion Act* (N.J.S.A. § 9:17A-1.1 through 1.12), was held unconstitutional in the case of *Planned Parenthood of Cent. New Jersey v. Farmer*, 165 N.J. 609, 762 A.2d 620 (2000).

- A minor who has or believes he/she has a sexually transmitted disease may consent to medical care or services without authorization by the minor's parent or legal guardian. (Reference: N.J.S.A. § 9:17A-4.) (Exception: See below regarding HIV/AIDS testing and treatment.)

- A minor who is at least 13 years old may consent to HIV/AIDS testing or treatment without authorization by his/her parent or legal guardian. (Reference: N.J.S.A. § 9:17A-4.)

- A minor who, in the judgment of a treating physician, appears to have been sexually assaulted, may consent to medical care without authorization by the minor's parent or legal guardian. However, the minor's parent or legal guardian shall be notified immediately, unless the attending physician believes that is in the best interests of the individual not to do so. Inability of the treating physician to locate the parents or guardian shall not preclude the provision of any necessary emergency medical care to the minor. (Reference: N.J.S.A. § 9:17A-4.)

- A minor who believes that he/she is suffering from the use of drugs or is a drug dependent person or is suffering from alcohol dependency or is an alcoholic may consent to medical care under the supervision of a licensed physician, without authorization by the minor's parent or legal guardian. (Reference: N.J.S.A. § 9:17A-4.)

- A minor over the age of 17 years may consent to donate blood in any voluntary and noncompensatory blood program without obtaining parental authorization. A minor over the age of 16 years may donate blood in any voluntary and noncompensatory blood program with the written consent of at least one parent or legal guardian. (Reference: N.J.S.A. § 9:17A-6.)

- Notwithstanding any of the above, under N.J.S.A. § 9:17A-5, a treating physician may, but is not obligated to, inform the minor's parent or legal guardian as to medical treatment given or needed for the minor. Such information may be given to, or withheld from, the parent or legal guardian without the consent of the minor and even over the express refusal of the minor to the providing of such information. (Reference: N.J.S.A. § 9:17A-5.)
    - Comment: Because a minor who has legal authority to consent to specific treatment generally controls the release of information regarding such treatment, physicians should use caution when releasing information to parents or guardians in reliance on this statutory provision, using the physician's best judgment. However, it should be noted that certain highly sensitive information, such as information concerning drug and alcohol abuse treatment and diagnosis and treatment related to HIV/AIDS, contain heightened protections under federal and state law. As such, this information should not be released except in compliance with such laws.

- Consent issues with regard to the child welfare system—including county child and youth agencies, child residential facilities, private foster care agencies, foster parents and the

dependency court—are not discussed here. Likewise, consent issues with regard to the delinquency system are not discussed here.

- Commentary: Physicians may offer confidentiality to an adolescent minor, or be asked by a minor for confidentiality, in situations when the minor does not have the legal right to consent to his/her own medical treatment. There is no state law governing confidentiality, or the breaking of confidentiality, in these situations. It is best to consider each case on an individual basis. In general, physicians should maintain adolescents' confidentiality except when keeping silent would put the patient's life or health at risk. Physicians should explain to patients and their parents or legal guardians that they will respect adolescent confidentiality unless doing so would put the patient's life or health at risk. Notwithstanding the above, we should recognize that in most circumstances, it is preferable for parents or legal guardians to know about their adolescent children's health issues. Physicians should encourage and promote open communication between adolescent patients and their parents or legal guardians.

EXHIBIT F

PARTNERSHIP FOR CHILDREN OF ESSEX

Denial Letter
(TO INSPECT AND/OR COPY PHI)

Date: _____

Name: _____
Address: _____
_____

In accordance with the regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), we have determined that we are unable to honor your request to inspect and obtain a copy of your protected health information (PHI) for the following reason(s):

The following reasons are non-reviewable (which means you do not have the right to request a review of our denial, as further explained below):

[ ] We do not possess the information requested. We:
____ do not know where or what provider maintains this information
____ understand you may be able to obtain this information from:
_____

[ ] The Privacy Rule does not require us to permit you to inspect and obtain a copy of the requested information because it has been compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding.

[ ] The Privacy Rule does not require us to permit you to inspect and obtain a copy of the requested information because it is subject to or exempted by the Clinical Laboratory Improvements Amendments (CLIA) of 1988.

[ ] The Privacy Rule does not require us to permit you to inspect and obtain a copy of the requested information because the information was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

[ ] The Privacy Rule does not require us to permit you to inspect and obtain a copy of the requested information because the information was/is being created or obtained in the course of on-going research that includes treatment and you agreed to the denial of access when you consented to participate in the research. Your right of access will be reinstated upon the completion of the research.

[ ] The requested information is psychotherapy notes.

[ ] The requested information is contained in records subject to the federal Privacy Act, 5 U.S.C. § 552a, and this denial meets the requirements of that law. The Privacy Act of 1974 protects personal information about individuals held by the federal government.

The following reasons are reviewable, as further explained below:

[ ] A licensed healthcare professional has determined in his/her professional judgment that access to the requested information is reasonably likely to endanger your life or physical safety or the life or physical safety of another person.

[ ] The requested information makes reference to another person (who is not a health care provider) and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.

[ ] You are the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that furnishing the requested information to you is likely to cause substantial harm to the individual or another person.

If access to requested information has been denied for any of the "reviewable" reasons listed above, you have the right to have the denial reviewed by another licensed healthcare professional of the organization who did not participate in this denial. If you choose to have this denial reviewed, please submit a written request to our Privacy Officer at:

Partnership for Children of Essex
300 Broadacres Dr. 3rd fl.
Bloomfield, NJ 07003
Phone: 973-323-3000
Fax: 973-323-3015

Our Privacy Officer will respond with a written decision within a reasonable period of time whether or not to grant or deny access to your PHI as originally requested.

If you desire to file a written complaint concerning a denial, you may do so by writing to the Privacy Officer at the address set forth above. You also may send a written complaint to the Secretary of the U.S. Department of Health and Human Services at 200 Independence Ave., S.W., Room 615F, Washington, DC 20201

Very truly yours,

_____

Printed Name:
Title:

EXHIBIT G

Request to Restrict Use or Disclosure of Protected Health Information

I, _____, D.O.B. ____/____/____, request a restriction on the use or disclosure of my personal health information by **Partnership for Children of Essex** (the "Organization").

I understand that I can request that the Organization restrict the use and/or disclosure of my personal health information as it relates to treatment, payment, or health care operations. I would like the Organization to restrict the use and/or disclosure of the following health information in the following manner:

_____

_____

_____

I understand that, except in certain limited circumstances, the Organization is not required to agree to my request. If the Organization does agree to my request, the restriction will not apply if the use or disclosure of information is necessary to provide me with emergency treatment or is required by law.

I understand that the Organization may terminate the restriction if: (1) I agree to or request the termination in writing, (2) I orally agree to the termination and the oral agreement is documented, or (3) the Organization informs me that it is terminating the restriction.

_____ ____/____/____

Signature of Individual or Individual's Authorized Representative Date

Representative's Name and Authority: _____

EXHIBIT H

Disclosure Restriction (to Health Plans) Acknowledgement Form

I, _____ (Name) have asked **Partnership for Children of Essex** not to bill my insurance for a visit or service(s) provided on _____ _____ (date) to my insurance carrier.

I understand that by signing this acknowledgement:

- I may have the right to request the restriction of disclosure to my health plan. The organization's policy is to collect payment for all services provided up front and in full if the service(s) are not being billed to my insurance.

- I have chosen to restrict one or more of the service(s) provided to me today from your insurance carrier.

- I am responsible for payment today for the services that I am hereby restricting from my insurance carrier. I am also responsible for payment today of any applicable copay pertaining to today's visit.

- I will provide Partnership for Children of Essex with payment for the services I received in full today.

- I agree that should there be a problem with the method of payment I have provided I have forty-five (45) days from the date of service to provide the office with the payment in full. If I do not do this, the organization has the right to submit the service to my health plan for payment.

- Should information I have chosen to restrict need to be transmitted to another entity, I understand that it is my responsibility to notify that entity of my request to restrict the information.

Signed by: _____ _____

Signature of Individual or Legal Guardian | Date of Birth

_____ _____

Print Name of Legal Guardian | Relationship to Individual

EXHIBIT I

Request for Correction/Amendment of Protected Health Information

Name: _____ D.O.B. ____/____/____

Address: _____
_____

1. Please Check the Type of Entry to be amended:

☐ *Visit Note*	☐ *Prescription Information*
☐ *Order*	☐ *Patient History*
☐ *Report*	☐ *Other:* _____

Date of Entry: _____

2. Please explain how the entry is inaccurate or incomplete:

_____
_____
_____ (attach additional forms or pages as needed)

3. Please specify as to what the entry should say to be more accurate or complete:

_____
_____
_____

I understand that **Partnership for Children of Essex** (the "Organization") may deny my request for an amendment (1) if the request is not in writing or does not include a reason why the amendment is necessary; or (2) if the information (i) was not created by the Organization, unless I provide reasonable evidence that the creator of the information is no longer available to act on my requested amendment, (ii) is not part of my clinical or billing records maintained by the Organization, (iii) is not part of the information that I have a right to inspect and copy, or (iv) is already accurate and complete as determined by the Organization.

I understand that in the event the Organization accepts my request for an amendment, I will be informed of the amendment and the Organization will make reasonable efforts to inform the persons or entities that have received my protected health information.

I understand that in the event the Organization denies my request for an amendment, I will have an opportunity to file a written statement of disagreement to which the Organization may prepare a written statement of rebuttal. I understand that any disagreement and rebuttal will be attached to any future disclosures.

_____ Date:_____
Signature of Individual or Individual's Authorized Representative

Representative's Name and Authority:_____

For Office Use Only:

Amendment has been:

☐ Accepted ☐ Denied ☐ Partially Denied / Accept

Name: _____

Date of Amendment: _____

If denied (in whole or in part)*, check reason for denial:

- ☐ PHI was not created by this organization.
- ☐ PHI is not available to the individual for inspection in accordance with the law.
- ☐ PHI is not a part of individual's designated record set.
- ☐ PHI is accurate and complete.

Comments from healthcare provider who provided service:

_____

_____

_____

_____

_____ _____

Signature of Healthcare Provider Who Provided Service Date

Name of Staff Member Completing Form (Please Print): _____

Title: _____ Date: _____

* THE ORGANIZATION MUST INFORM INDIVIDUAL THAT A WRITTEN REQUEST IS REQUIRED, AND THAT THE INDIVIDUAL IS REQUIRED TO PROVIDE A REASON TO SUPPORT THE REQUESTED CHANGE.

EXHIBIT J

Request for an Accounting of Disclosures

Name:_____ D.O.B. ____/____/____

I hereby request that **Partnership for Children of Essex** provide me with an accounting that lists the disclosures of my **[circle if applicable: electronic]** protected health information (PHI) made by _____ from ____/____/____ through ____/____/____ (time period may not go back farther than 6 years from the date of this request and 3 years in the event the request is made for an accounting of electronic PHI).

I understand that this accounting will not include: (1) disclosures for purposes of treatment, payment or health care operations (except for accountings for electronic disclosures); (2) disclosures made directly to me or a family member; (3) disclosures made incident to a use or disclosure otherwise permitted or required by law; (4) disclosures made pursuant to my written authorization; (5) disclosures for a patient directory; (6) disclosures made for national security or intelligence purposes; or (7) disclosures to law enforcement officials.

I understand that I am entitled to receive an accounting free of charge every 12 months. I understand that I may be charged for any additional accounting requests during the same 12 month period. I also understand that I will be made aware of any charges and given the opportunity to withdraw or modify the request for an accounting prior to being charged for the additional accounting.

Please mail (or, if applicable, email) the information to me at:

_____
_____
_____

I understand that _____ has sixty (60) days to respond to this request.

_____ _____/_____/_____
Signature of Individual or Authorized Representative Date

Representative's Name and Authority:_____

EXHIBIT K

Accounting of Disclosure Record for Protected Health Information

[Note: If the organization's medical record system is capable of tracking accountings of disclosures, the attached form is unnecessary.]

Name:_____ D.O.B.____/____/____

Accounting Period from ____/____/____ through ____/____/____

For each program participant, you are required to keep a log of all disclosures of PHI for non-TPO reasons for which you did not receive a signed authorization from the individual. For each disclosure, fill in the date occurred along with a description of the type of disclosure. In addition, you need to provide a description of the PHI disclosed along with the names and titles to whom it was disclosed. The Organization must retain related documentation and a tracking log for each program participant for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

Date*	Basis for Disclosure	Information Disclosed	Who Requested Disclosure	Name/Address to Whom Disclosed

*For multiple disclosures to a single person or entity made for a single purpose, record the information as required for the first disclosure, record the frequency of disclosures made during the time period involved and record the date of the last disclosure made during this accounting period.

EXHIBIT L

Partnership for Children of Essex

Health Privacy Complaint Form

Today's Date: ____/____/____

Name:_____ D.O.B.: _____/_____/_____

Address: _____
_____
_____

Telephone Number (____) _____-_____

Please describe the acts or omissions that you believe to be a violation of your privacy rights under privacy laws (attach additional sheets as necessary):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Date(s) that the above described acts or omissions occurred: _____

Please submit this complaint form to us at the following address:

_____
_____
_____
Attn: Privacy Officer

Thank you for taking the time to provide us with this information. You also have the right to file your complaint with the Secretary of the U.S. Department of Health and Human Services as set forth in our Notice of Privacy Practices.

EXHIBIT M

Partnership for Children of Essex

Documentation of Privacy Complaints by Privacy Officer

Date of Complaint: ____/____/____

Program Participant:_____ D.O.B.: ____/____/____

Complaint was received: _____ Orally _____ In Writing (attached to this form)

Nature of complaint or additional information gathered (attach additional pages as necessary)

_____
_____
_____
_____
_____

Results of investigation of complaint:

_____
_____

In the event the investigation revealed a violation of the individual's privacy rights:

- If complaint was against workforce member or other member of workforce, describe any sanctions that were taken against the workforce member or member of workforce:

  _____
  _____

- If complaint was against business associate describe actions taken:

  _____ Business associate was contacted and agreed to the following:
  _____
  _____

  _____ Business associate was contacted, but refused to make changes to cure the breach.
  _____ Agreement with business associate was terminated
  _____ Determination was made that there were no options other than using this business associate and the Secretary of the U.S. Department of Health and Human Services was contacted (attach letter to Secretary)

List any steps that were taken to mitigate past or future harm to the individual:

_____
_____

EXHIBIT N

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (this "Agreement") is made as of the date set forth below on the signature page by and between the following parties (each a "Party" and collectively the "Parties"):

Partnership for Children of Essex, with offices at 300 Broadacres Drive, 3rd Floor, Bloomfield, New Jersey 07003 ("Covered Entity")

and

_____, with offices at _____ ("Business Associate").

WITNESSETH:

WHEREAS, Business Associate has entered into an agreement with Covered Entity to provide services, the performance of which may require Business Associate to have access to Protected Health Information (as defined below) concerning patients of Covered Entity (the "Services"); and

WHEREAS, Covered Entity and Business Associate intend to meet their obligations regarding the use and disclosure of Protected Health Information under the federal Health Insurance Portability and Accountability Act of 1996 ("Original HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH," and collectively with Original HIPAA, the "HIPAA Statute"), along with regulations promulgated by the Secretary of the Department of Health & Human Services ("HHS") under the HIPAA Statute, including the "Privacy Rule" (45 C.F.R. Parts 160 and 164, Subparts A and E) and the "Security Rule" (45 C.F.R. Part 160 and 164, Subparts A and C), as amended by the "Omnibus Rule" (45 C.F.R. Part 160, Subparts A, B, C and D and Part 164, Subparts A and C) (the Privacy Rule, the Security Rule and the Omnibus Rule, collectively the "HIPAA Rules"), as well as any other applicable laws concerning the privacy and security of health information, all as may be amended from time to time (collectively referred to herein as "HIPAA").

NOW, THEREFORE, intending to be legally bound, the Parties hereto agree as follows:

1. **Entire Agreement.** This Agreement represents the entire agreement and understanding of the Parties with respect to the subject matter hereof, and it supersedes any prior or current oral or written business associate agreement between the Parties.

2. **Definitions.**

(a) Interpretation. The terms defined below are included for ease of reference and are intended to have the same meaning as provided under HIPAA. Other terms used but not otherwise defined in this Agreement are also intended to be defined and interpreted in accordance with HIPAA.

(b) "Breach." The term "Breach" means, as defined in 45 CFR § 164.402, the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information.

(c) "Designated Record Set." The term "Designated Record Set" means, as defined in 45 CFR § 164.501, a group of records maintained by or for a covered entity that is, (i) the medical records and billing records about individuals maintained by or for a covered health care provider, or (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan, or (iii) used, in whole or in part, by or for a covered entity to make decisions about individuals. For purposes of this paragraph, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

(d) "Electronic Protected Health Information." The term "Electronic Protected Health Information" (also "E-PHI") means, as defined in 45 CFR § 160.103, individually identifiable health information that is transmitted by or maintained in electronic media.

(e) "Protected Health Information." The term "Protected Health Information" (also "PHI") means, as defined in 45 CFR § 160.103, information that, (i) is created or received by a health care provider, health plan, employer or health care clearinghouse, (ii) relates to the past, present, or future physical or mental condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual, and (iii) either identifies an individual or there is a reasonable basis to believe that it could be used to identify an individual.

(f) "Required by Law." The phrase "Required by Law" means, as defined in 45 CFR § 164.103, a mandate contained in law that compels an entity to make a use or disclosure of Protected Health Information and that is enforceable in a court of law. Required by Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, a grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; civil or authorized investigative demands; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

(g) "Secretary." The term "Secretary" means, as defined in 45 CFR § 160.103, the Secretary of the Department of Health and Human Services or any other officer or employee of the department to whom the authority involved has been delegated.

(h) "Security Incident." The term "Security Incident" means, as defined in 45 CFR § 164.304, the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with system operations in an information system.

(i) "Subcontractor." The term "Subcontractor" means, as defined in 45 CFR § 160.103, a person to whom Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of Business Associate.

(j) "Unsecured PHI." The term "Unsecured PHI" means, as defined in 45 CFR § 164.402, PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary.

3. **Permitted Uses and Disclosures of PHI.**

(a) Performance of Services. Except as otherwise prohibited or limited by any applicable law, rule or regulation, Business Associate may use or disclose PHI to perform the Services for or on behalf of Covered Entity, provided that (i) such use or disclosure involves only the minimum amount of PHI as is necessary for such performance, and (ii) the use or disclosure would not violate HIPAA if done by Covered Entity.

(b) Subcontractors. Business Associate may disclose PHI to a business associate (as defined in 45 CFR § 160.103) that is a Subcontractor and may permit such Subcontractor to create, receive, maintain or transmit PHI, including E-PHI, on its behalf, but only if Business Associate enters into a written business associate agreement with the Subcontractor that satisfies the requirements of 45 CFR § 164.314(a) and § 164.504(e).

(c) Management, Administration and Legal Responsibilities. Business Associate may use PHI as is necessary for the proper management and administration of Business Associate or for Business Associate to perform its legal obligations. Business Associate may disclose PHI for such purposes, but only if (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any breach of confidentiality concerning such information of which it is aware.

(d) Data Aggregation Services. Except as otherwise set forth herein, Business Associate may use PHI to provide data aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B), so long as such services are within the scope of Services under the agreement for Services and provided consistent therewith.

(e) Reporting. Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR § 164.502(j)(1).

4. **Responsibilities of the Parties with Respect to PHI.**

(a) Obligations and Activities of Business Associate.

(i) Business Associate shall not use or disclose PHI other than as permitted or required under this Agreement, or as Required by Law.

(ii) Business Associate shall use appropriate administrative, physical and technical safeguards and comply with the applicable requirements of Subpart C of 45 CFR § 164 with respect to E-PHI to prevent the use or disclosure of PHI other than as provided for herein.

(iii) Business Associate shall comply with the applicable requirements of Subpart E of 45 CFR § 164. To the extent that Business Associate, in providing the Services,

is carrying out one or more of Covered Entity's obligations under Subpart E of 45 CFR § 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

(iv) Business Associate shall ensure that any Subcontractors that create, receive, maintain or transmit PHI, including any E-PHI, on behalf of Business Associate agree to comply with the applicable requirements of Subpart C and Subpart E of 45 CFR § 164, and that each Subcontractor enters into a business associate agreement with Business Associate under which each Subcontractor agrees to the same restrictions and conditions that apply to Business Associate with respect to PHI. In addition to other provisions required by HIPAA or this Agreement, such Subcontractor agreements shall contain provisions to ensure Business Associate will meet its reporting obligations under **Sections 4(a)(v)** and **4(a)(vi)**, immediately below.

(v) Business Associate shall promptly report to Covered Entity, within five (5) business days of discovery, any use or disclosure of PHI not permitted by this Agreement, as well as any successful Security Incident. In addition, Business Associate shall promptly and without unreasonable delay, notify Covered Entity following the discovery of a Breach of Unsecured PHI as required by 45 CFR § 164.410, except that Business Associate shall make such reports to Covered Entity no later than five (5) business days after discovery of the same unless a law enforcement official determines that such a report would impede a criminal investigation or cause damage to national security, in which case Business Associate will comply with 45 CFR § 164.412. A Breach is deemed discovered as of the first day on which it is known to Business Associate or to any person, other than the person committing the Breach, who is an employee, officer or other agent of Business Associate, or, by exercising reasonable diligence, would have been known to Business Associate or such person.

(vi) Business Associate shall include in any report required under **Section 4(a)(v)** immediately above, to the extent possible, (A) a description of and details concerning the impermissible use/disclosure, successful Security Incident or Breach of Unsecured PHI, including the date of discovery by Business Associate (B) the identification of each individual whose PHI has been, or is reasonably believed to have been, the subject of the impermissible use/disclosure, Security Incident or Breach of Unsecured PHI, (C) a description of the Business Associate's investigation into the impermissible use/disclosure, Security Incident or Breach of Unsecured PHI, including mitigating actions taken by Business Associate to mitigate harm to affected individuals and protect against further breach; (D) contact information for the individual within Business Associate's organization most knowledgeable about the impermissible use/disclosure Security Incident or Breach of Unsecured PHI and who is responsible for coordinating efforts with Covered Entity with respect to same, and (E) such other available information, as requested by Covered Entity, which Covered Entity may be required to include in any required notifications to the affected individuals.

(vii) Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of (A) a successful Security Incident, (B) a Breach of Unsecured PHI, and (C) a use or disclosure of PHI by Business Associate or its employees or agents, including any Subcontractors, in violation of the requirements of this Agreement. Further, Business Associate shall reasonably cooperate and coordinate with Covered

Entity in the investigation of any violation of the requirements of this Agreement, including any impermissible use/disclosure, Security Incident or Breach of Unsecured PHI.

(viii) Business Associate, within ten (10) business days after written request by Covered Entity, shall provide access to PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an individual in order to meet the requirements under 45 CFR § 164.524.

(ix) Within ten (10) business days after written request by Covered Entity, Business Associate shall make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR § 164.526.

(x) Within ten (10) business days after written request by Covered Entity, Business Associate shall make available to Covered Entity information required to provide an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

(xi) Within five (5) business days after written request by Covered Entity, Business Associate shall make internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to Covered Entity and the Secretary for purposes of Covered Entity's or the Secretary's determination of the Parties' compliance with HIPAA.

(xii) If the scope of Services includes electronic transactions, Business Associate shall satisfy all applicable provisions of the HIPAA standards for electronic transactions and code sets, also known as the Electronic Data Interchange (EDI) Standards, codified at 45 C.F.R. Part 162. Business Associate further agrees to ensure that any Subcontractor that conducts standard transactions, as such term is defined at 45 C.F.R. § 162.103, on its behalf will comply with the EDI standards.

(b) Obligations of Covered Entity.

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

(ii) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

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

5. **Term and Termination.**

(a) Term. This Agreement is effective as of the date first set forth below, and continues in effect until otherwise terminated in accordance with this **Section 5**.

(b) Termination.

(i) If either Party knows of a pattern of activity or practice of the other Party that constitutes a material breach or violation of this Agreement, then the Party shall provide written notice of the breach or violation to the other Party that specifies the nature of the breach or violation. The breaching Party must cure the breach or end the violation on or before thirty (30) days after receipt of the written notice. In the absence of a cure reasonably satisfactory to the non-breaching Party within the specified time frame, or in the event the breach is reasonably incapable of cure, then the non-breaching Party may do the following:

(A) if feasible, terminate this Agreement and any and all agreements for Services; or

(B) if termination of this Agreement or the agreements for Services is infeasible, report the issue to the Department of Health and Human Services.

(ii) Notwithstanding the foregoing, Covered Entity may immediately terminate this Agreement and any and all agreements for Services if Covered Entity determines that Business Associate has breached a material term of this Agreement and no cure is possible.

(c) Automatic Termination. This Agreement automatically terminates without any further action of the Parties, (i) if the Services are no longer provided by Business Associate to or on behalf of Covered Entity, or (ii) if HIPAA is no longer applicable to Covered Entity.

(d) Obligations of Business Associate upon Termination, Expiration or Non-Renewal.

(i) Return or Destruction. Upon the expiration, termination or non-renewal of this Agreement, for any reason, Business Associate shall return or destroy all PHI (including E-PHI) received from, or created or received by, Business Associate on behalf of Covered Entity that Business Associate still maintains in any form, and shall retain no copies of such PHI (including E-PHI), unless such return or destruction is not feasible.

(ii) Non-Return or Destruction. If it is not feasible for Business Associate to return or destroy the PHI (including E-PHI) upon the termination of this Agreement for any reason, as reasonably determined in good faith by Business Associate, Business Associate shall extend indefinitely any and all protections, limitations and restrictions contained in this Agreement to its use and disclosure of such PHI (including E-PHI).

6. **Indemnification.**

(a) Indemnification of Covered Entity. Business Associate agrees to and shall indemnify and hold harmless Covered Entity from and against any and all losses, damages, liabilities, demands and claims of any nature whatsoever, including reasonable legal fees and costs (collectively, "Losses") arising out of, based upon, resulting from or in any way relating to any act or omission of Business Associate (to include Business Associate and its principals, officers, directors, employees, agents, independent contractors and Subcontractors) in violation of this Agreement or that in any way otherwise constitutes or directly or indirectly causes or results in

any use or disclosure not permitted by this Agreement, any Security Incident and any Breach of Unsecured PHI. For purposes of this Agreement, Losses shall include, but not be limited to, costs of investigation, mitigation, credit monitoring, notifications, penalties and fines. Business Associate agrees to and shall reimburse Covered Entity for any and all Losses immediately upon demand by Covered Entity.

(b) Business Associate Losses. Business Associate shall be responsible for, and shall at its own expense, defend itself against any and all losses, damages, liabilities, demands and claims of whatever kind or nature, arising out of or in connection with any act or omission of Business Associate (to include Business Associate and its principals, officers, directors, employees, agents, independent contractors and Subcontractors) in the performance of the duties and obligations of Business Associate under the Services agreement or this Agreement ("BA Losses"). Business Associate hereby releases and hold harmless Covered Entity from any and all BA Losses.

(c) Unaffected by Limitations. The provisions of this **Section 6** shall control and be unaffected by any limitation of remedies that may be contained in any agreement for Services between the Parties.

7. **Miscellaneous.**

(a) Survival. The provisions of **Section 5(d)**, **Section 6** and **Section 7** survive the expiration or termination of this Agreement for any reason.

(b) Independent Contractor. Business Associate and Covered Entity are independent contractors. Nothing in this Agreement may be deemed or construed by the Parties hereto or by any third party as creating the relationship of employer and employee, principal and agent, partners, joint ventures, or any similar relationship, between the Parties. Except as expressly set forth herein, the Parties to this Agreement do not intend, nor shall anything in this Agreement be construed, to create any rights in any third parties.

(c) Amendments; Waiver. This Agreement may not be modified, nor may any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event may not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

(d) Counterparts. This Agreement may be executed in multiple, identical counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument. Signatures of this Agreement transmitted by facsimile transmission, by electronic mail in "portable document format" (".pdf") form, or by any other electronic means intended to preserve the original graphic and pictorial appearance of a document, will have the same effect as physical delivery of the paper document bearing the original signature.

(e) Further Assurances. Each Party shall do all acts, and make, execute and deliver such written instruments as may from time to time be reasonably required to carry out the terms, conditions and provisions of HIPAA, as promulgated from time to time.

(f) Severability. If any provision of this Agreement or the application thereof to any person, entity, or circumstance is found, for any reason or to any extent, to be invalid or unenforceable by a court of competent jurisdiction or government agency with the authority to make such a finding, the remainder of this Agreement and the application hereof to any person, entity or circumstance will not be affected thereby, but rather the remainder of this Agreement will be enforced to the greatest extent permitted by law.

(g) Choice of Law; Jurisdiction. This Agreement is governed by, and should be construed in accordance with, the laws of the State of New Jersey. The Parties consent to the filing of an action in, and hereby personally submit to the jurisdiction of, the state or federal courts located in the State of New Jersey.

(h) Benefit. This Agreement is binding upon and inures to the benefit of the Parties hereto, their respective heirs, executors, administrators, successors and permitted assigns.

(i) Assignment. Except as otherwise provided herein, this Agreement and the obligations, rights and benefits hereunder may not be assigned by either Party without the prior written consent of the other Party.

(j) Headings. The paragraph headings in this Agreement are solely for convenience or reference and are not intended to affect its interpretation.

(k) Notice. Whenever, under the provisions of this Agreement, notice is required to be given, it will be in writing and will be deemed given three (3) business days after being mailed, certified or registered mail, return receipt requested, or one (1) business day after deposit with a nationally recognized overnight courier, addressed to the Parties at the addresses set forth above, or when given by hand delivery.

(l) Regulatory References. A reference in this Agreement to a section in HIPAA means the section as in effect or as amended.

(m) Construction. It is specifically understood and agreed by and between the Parties that this Agreement is the result of negotiations between the Parties. Accordingly, it is understood and agreed that all Parties will be deemed to have drawn these documents and there will be no negative inference from the language of this Agreement by any fact finders as against any Party.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, each of the undersigned has caused this Business Associate Agreement to be duly executed in its name and on its behalf on the date set forth below.

COVERED ENTITY **PARTNERSHIP FOR CHILDREN OF ESSEX**	**BUSINESS ASSOCIATE** _____
By: _____	By: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____