HIPAA PRIVACY POLICIES

Brittany Quagan, PLLC (Provider) complies with federal and state laws governing privacy and confidentiality of patients' health information as detailed in the sections of this Policy.

Table of Contents

I. Definitions (§ 164.501)

A. Business Associate – An outside entity or person that performs work on Provider's behalf and requires access to or the use or disclosure of protected health information (PHI) to perform the work. Examples of such work include but are not limited to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management and practice management as well as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

B. Disclosure - The release, transfer, provision of access to, or divulging in any other manner of PHI outside Provider.

C. Individually Identifiable Health Information - Information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by Provider; and

2. Relates to the past, present, or future physical or behavioral health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

    a. That identifies the individual; or

    b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual

D. Patient - The patient or his/her Personal Representative.

E. Personal Representative - A person who, under applicable state law, has the authority to act on behalf of an individual in making decisions related to health care.

F. Privacy Officer - The person appointed by Provider to serve as Privacy Officer or his/her designee.

G. Protected health information (PHI) - Individually identifiable health information that Provider maintains on patients except for: (1) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; (2) Student records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (3) Employment records held by Provider in its role as employer.

H. Required by law - A mandate contained in law that compels Provider to make a use or disclosure of PHI and that is enforceable in a court of law.

I. Use - With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within Provider.

II. Uses and disclosures of PHI

A. General rules (§164.502)

It is Provider's policy to use or disclose a patient's PHI only as permitted by law and in accordance with our Notice of Privacy Practices and to adopt safeguards to preserve the confidentiality of our patients' PHI.

Provider shall obtain an Authorization from the patient that complies with Provider's policy on "Authorizations" prior to using or disclosing a patient's PHI except where state and federal law specifically permit the proposed use or disclosure, as outlined in these Policies. Questions regarding the permissibility or conditions of a use or disclosure of PHI must be directed to the Privacy Officer.

B. Business Associates. (§164.504)

Disclosures by Provider to Business Associates[1] are made only pursuant to written agreements regarding privacy and confidentiality that comply with federal and state law (Business Associate Agreement or BAA). Such BAA must contain satisfactory assurances that the Business Associate will appropriately safeguard PHI and will not use or disclose such information in a manner that would violate the requirements of federal or state law. The Privacy Officer is responsible for ensuring that BAAs are obtained where necessary.

C. Treatment, Payment, or Health Care Operations (§164.506)

Treatment. Provider uses or discloses patients' PHI for treatment purposes without an Authorization when the following definition of treatment applies:

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

Payment. Provider uses or discloses patients' PHI for payment purposes without an Authorization when the following definition of payment applies:

1. The activities undertaken by Provider to obtain reimbursement for the provision of health care; and

2. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:
   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. Risk adjusting amounts due based on enrollee health status and demographic characteristics;
   c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
   d. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
   e. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
   f. Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: (i) Name and address; (ii) Date of birth; (iii)

[1] Independent contractors who provide treatment are not Business Associates. An independent contractor who provides treatment and performs services on behalf of Provider that requires the use of PHI is a Business Associate.

Social security number; (iv) Payment history; (v) Account number; and (vi) Name and address of the health care provider and/or health plan.

Health Care Operations of Other Providers. Provider *discloses* a patient's PHI to another health care provider or covered entity for that provider's or covered entity's health care operations only if: (i) Provider and the entity to which the information is disclosed have or had a relationship with the patient whose information is being disclosed; and (ii) the disclosure is for a purpose described below; or (iii) the disclosure is for the purpose of health care fraud and abuse detection or compliance. Provider *uses* patients' PHI for all health care operations as described below.

Deleted: ies

Deleted: in Paragraph 4(c)(1) or 4(c)(2)

1. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care lean under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

3. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

4. Business planning and development; and

5. Business management and general administrative activities of Provider.

D. Uses and disclosures Requiring an Authorization (§164.508)

All uses and disclosures not otherwise permitted under this Section II require a written Authorization signed by the patient. Provider has an Authorization form that complies with HIPAA requirements. All Authorizations must be maintained in the patient's record. Questions about whether Authorizations from other sources meet HIPAA requirements must be directed to the Privacy Officer.

Disclosures pursuant to an Authorization must strictly adhere to the limitations on scope detailed in the Authorization. If a cover letter requests a narrower scope of information than noted in the Authorization, provide only the information requested in the cover letter. A cover letter, however, cannot expand the scope of Authorization.

[if you plan to use PHI for marketing or sales, you need additional language here]

E. Opportunity for the individual to agree or to object (§164.510)

Provider may disclose PHI without an Authorization to a person involved in the patient's health care to the extent of their involvement or to notify a family member, legal guardian or Personal Representative of the patient's location, general condition or death, provided that prior to disclosing

PHI, Provider provides the patient and/or the Personal Representative with an opportunity to agree or object and to prohibit or restrict such disclosures. Agreement can be inferred from circumstances based on Provider's exercise of professional judgment when the patient expresses no objection (e.g., brings a family member into an exam room). If the patient is not able to agree or object due to incapacity or in emergencies, Provider can act in the best interest of the patient based on professional judgment. Involved in care disclosures are also permitted after a patient's death to the extent of the person's involvement.

F. No opportunity to agree or object is required (§164.512)

1. Uses and Disclosures Required by Law - Provider may use and disclose PHI to the extent the use or disclosure is required by law and limits the use or disclosure to the relevant requirements of the law. All requests for disclosures of PHI required by law should be referred to the Privacy Officer.

2. Uses and Disclosures for Public Health Activities - (1) Public Health Authority. Provider may report disease, vital events such as birth or death and the conduct of public health surveillance, public health investigations, and public health interventions to a public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability. (2) Abuse or Neglect. Provider may disclose PHI to a public health authority or other appropriate government authority authorized by law to receive reports of child, elder or developmentally disabled individual abuse or neglect. (3) FDA. Provider may disclose PHI with respect to an FDA regulated product or activity related to the quality, safety or effectiveness of the FDA regulated product or activity. (4) Employer. Provider may disclose PHI consisting of findings concerning a work-related illness or injury or workplace-related medical surveillance to an employer, about a person who is a member of the workforce of the employer, under limited circumstances. Involve the Privacy Officer with questions or concerns.

3. Disclosures about victims of abuse, neglect or domestic violence - Provider is a mandated reporter of suspected abuse and neglect. Disclosures made for purposes of reporting child, elder and/or developmentally disabled abuse or neglect shall be made in accordance state law. If other laws permit the disclosure of information related to domestic violence, Provider may disclose information if: (1) Provider believes, in its professional judgment, that the disclosure is necessary to prevent serious harm to the patient or other potential victims; or (2) If the individual is unable to agree because of incapacity, a law enforcement or other public official represents that the PHI is not intended to be used against the individual and that immediate enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

   If such disclosure is made, Provider shall be responsible for promptly informing the patient unless: (1) Provider determines, in the exercise of professional judgment, that informing the patient would place the patient at risk of serious harm; or (2) Provider would be informing a Personal Representative and reasonably believes the Personal Representative is responsible for the abuse, neglect or other injury and determines that informing that person would not be in the best interests of the patient.

4. Uses and Disclosures for Health Oversight Activities - Provider may use or disclose PHI to a health oversight agency for oversight activities authorized by law including audits by state agencies and their authorized representatives; civil, administrative or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative or criminal proceedings or actions by a health oversight agency; or other activities necessary for appropriate oversight of the health care system, and determining compliance with government benefit programs. Provider does not make disclosures of a patient's PHI pursuant to this Policy for investigations or other activities in which the patient is the subject of the investigation and the investigation does not arise out of and is not directly related to the patient's care or access to public benefits or services.

Deleted: assess

5. Disclosures for Judicial and Administrative Proceedings - Provider may disclose PHI in response to a request made in connection with a judicial or administrative proceeding when the request is accompanied by a valid Authorization. If the request, including a subpoena, is not accompanied by a valid Authorization, Provider will only disclose the requested PHI if the request is accompanied by an order of a court of competent jurisdiction directing the disclosure. The Privacy Officer will participate in disclosure decisions where there is no Authorization. HIPAA rules permit disclosure under circumstances where "satisfactory assurances" are provided, however, Provider is not required to disclose based on such satisfactory assurances. Generally, Provider will not accept satisfactory assurances but rather will insist on an Authorization or court order. Any exceptions must be approved by the Privacy Officer.

6. Disclosures for Law Enforcement Purposes

   a. *Pursuant to Process and as Otherwise Required by Law* – Examples include reporting of certain wounds, court-ordered warrant, grand jury subpoena, administrative request tied to a legitimate law enforcement inquiry which is specific and limited in scope and where de-identified information could not reasonably be used.

   b. *Limited Information for Identification and Location Purposes* - Provider may disclose PHI to a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person except that Provider may not disclose PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue. Further, any disclosed information must be limited to: (i) Name and address; (ii) Date and place of birth; (iii) Social Security number; (iv) ABO blood type and rh factor; (v) Type of injury; (vi) Date and time of treatment; (vi) Date and time of death, if applicable; and (vii) A description of distinguishing physical characteristics (e.g., height, weight, gender, race, hair and eye color, facial hair, scars, tattoos etc.).

   c. *Victims of Crime*. Except for disclosures required by law and disclosures about victims of abuse, neglect or domestic violence or child abuse or neglect (see II.F.3 of this Policy), Provider may disclose PHI about a patient who is suspected to be a victim of a crime only if: (i) the patient agrees to the disclosure; or (ii) where the patient's agreement cannot be obtained because of incapacity or other emergency circumstance and (a) such information is needed to determine whether a violation of law by another person has occurred and such information is not intended to be used against the victim patient; or (b) immediate law enforcement activity that depends on the disclosure would be materially and

adversely affected by waiting until the patient is able to agree to the disclosure; and the disclosure is in the best interests of the patient as determined by Provider in the exercise of professional judgment.

d. *Decedents.* Provider 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 Provider has a suspicion that such death may have resulted from criminal conduct.

e. *Crime on the Premises.* Provider may disclose to a law enforcement official PHI that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on Provider's premises.

f. *Reporting Crime in Emergencies.* Where Provider is providing emergency health care in response to a medical emergency at a location other than on Provider's premises, Provider may disclose PHI to law enforcement if it appears necessary to alert them to the commission and nature of a crime; the location of such crime or the victims of such crime; and the identity, description and location of the perpetrator of such crime.

7. Disclosures About Decedents. (1) Coroners and Medical Examiners. Provider may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or for other duties as authorized by law. (2) Funeral Directors. Provider may disclose PHI to funeral directors, consistent with applicable law, as necessary for them to carry out their duties with respect to the decedent. If necessary, Provider may disclose PHI prior to, and in reasonable anticipation of, the patient's death.

8. Uses and disclosures for research purposes. Provider may use or disclose PHI for research purposes without a patient's Authorization only if Provider complies with the requirements in HIPAA. All uses or disclosures for research purposes must be approved by the Privacy Officer.

9. Uses and Disclosures to Avert Serious Threat to Health or Safety. Provider may use or disclose PHI if Provider determines in good faith that the use or disclosure: (1) is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and the disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or (2) is necessary for law enforcement authorities to identify or apprehend an individual who has made a statement admitting participation in a violent crime that Provider reasonably believes may have caused serious physical harm to the victim (disclosure must be limited to the statement); or where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

   Provider shall not make a use or disclosure under (2) above if the information is learned by Provider during a counseling or therapy session or if the information is learned during treatment to affect the propensity to commit the violent crimes that are described in the individual's statements. Any disclosure under (2) must be limited to: (i) Name and address; (ii) Date and place of birth; (iii) Social Security number; (iv) ABO blood type and rh factor; (v) Type of injury; (vi) Date and time of treatment; (vi)Date and time of death, if applicable; and (vii) A description of distinguishing physical characteristics (e.g., height, weight, gender, race, hair and eye color, facial hair, scars, tattoos etc.).

10. Uses and Disclosures for Specialized Government Functions. Provider may use or disclose PHI for specialized government functions without an Authorization for the following: military and veterans activities, national security and intelligence activities, protection services for the president and others, correctional institutions and other law enforcement custodial situations. The Privacy Officer must be consulted prior to making disclosures for specialized government functions.

11. Disclosures for Workers' Compensation. Provider may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

G. Other requirements (§164.514)

1. De-identification of PHI. Provider is free to use and disclose PHI (PHI) that has been de-identified for research, demographics or other uses. The Privacy Officer should be consulted about the use of de-identified data. Any disclosure of de-identified information is reviewed by the Privacy Officer to ensure compliance with this Policy.

2. Minimum Necessary. Provider will make reasonable efforts to limit disclosures of PHI to the minimum amount reasonably necessary to achieve the intended purpose of the disclosure, except for: (a) disclosures required by law, (b) disclosures to health care providers for treatment purposes, (c) disclosures pursuant to an Authorization or disclosures to the patient, and/or (d) disclosures to the Secretary of HHS.

3. Limited Data Set. Provider may use or disclose a limited data set as defined under HIPAA, if Provider enters into a data use agreement with the limited data set recipient that meets the requirements in HIPAA. Any use of a limited data set and data use agreement must be approved by the Privacy Officer.

4. Fundraising Communications. Provider will not use PHI for fundraising purposes.

5. Verification Requirements. If the identity or authority of any person requesting PHI is not known to Provider, Provider will take reasonable steps to verify that person's identity and/or authority. If there is a reasonable doubt regarding the validity, the Privacy Officer should be notified immediately. The Privacy Officer shall investigate and resolve any issues related to verification. The authority of a Personal Representative other than natural or legal parent must be confirmed through appropriate legal documents or court orders and those documents must be maintained in the record.

   To verify the identity of public officials, provider may rely on: (1) presentation of an agency identification badge, other official credentials, or proof of government status; (2) a request made on the appropriate government letterhead; or (3) a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation that establishes that the person is acting on behalf of the public official. To verify the authority of public officials, Provider may rely on: (1) A written statement attesting to such legal authority or an oral statement when provision of a written statement is impracticable; or (2) A request made pursuant to legal process, warrant, order, or other legal process issued by a court or administrative tribunal.

Deleted: and/or (e) disclosures required by law

Deleted: use

III. Notice of Privacy Practices for PHI (§ 164.520)

It is the Policy of Provider to provide a written Notice of Privacy Practices to all patients and to other persons upon request, which outlines possible uses and disclosures of the patient's PHI and Provider's duties with respect to such information. A Notice of Privacy Practices shall be provided to all patients at or before the time of first service delivery, or as soon as practicable thereafter in the event of an emergency. A copy of Provider's Notice of Privacy Practices shall be conspicuously posted within the various locations of Provider and on its website. Provider shall make a good faith effort to obtain a signed written acknowledgement of receipt of the Notice of Privacy Practices on the form provided by Provider. A copy of the written acknowledgment shall be kept in the patient's health record. A copy of Provider's Privacy Notice, including copies of any updated Notices, will be retained by Provider for a period of six (6) years or any longer if the Notice is included in the patient's health record.

IV. Patient Rights

A. Request Restrictions on Uses and Disclosures of PHI (§164.522(a))

Provider recognizes a patient's right to request that Provider restrict uses or disclosures of PHI about the patient to carry out treatment, payment or health care operations. Provider is not required, however, to agree to a patient's request for restriction except that Provider must comply with the requested restriction if: (1) the disclosure is to a health plan for purposes of carrying out payment or health care operations, except as otherwise required by law; and (2) the PHI pertains solely to a health care item or service for which Provider has been paid out of pocket in full.

If Provider agrees to a requested restriction, Provider shall not use or disclose PHI in violation of the restriction except where the information is needed to provide the patient with emergency treatment and Provider will request that the emergency treating provider not disclose the information.

Disclosures required by law shall be made by Provider regardless of any requested restrictions by the patient.

Provider may terminate its agreement to a restriction if: (1) the patient agrees to or requests the termination in writing; (2) the patient orally agrees to the termination and the oral agreement is documented; or (3) Provider informs the patient that it is terminating its agreement to a restriction, except that the termination will be effective only with respect to PHI created or received after Provider has informed the patient that is terminating the restriction.

B. Request Confidential Communications (§164.522(b))

All patients have the right to request to receive confidential communications by alternative means or at an alternative address. Provider will accommodate reasonable requests by patients to receive confidential communications. Patients are not required to provide Provider with an explanation for the request for confidential communications as a condition of providing confidential communications. Provider may refuse to grant a request for confidential communication if the patient refuses to specify an alternate address or method of contact or refuses to provide information as to how payment, if any, will be handled.

C. Access to PHI (§164.524)

1. Generally. Subject to limited exceptions, Patients and Personal Representatives are entitled to access to patient's records that are maintained in a Designated Record Set without the need to execute an Authorization, although Provider may request that the patient's request be in writing. The right to access does not apply to psychotherapy notes (although Provider does not maintain psychotherapy notes), or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

2. Making the Request. If a Patient or his or her Personal Representative requests to access his or her record, the individual must make such request in writing detailing the type of access (inspection or copies), the specific records requested and, if copies are requested, specify paper or electronic copies and details for delivery. A complete Authorization form is not required and Provider will not require all of the information collected on the Authorization form if patient makes the request on an Authorization form.

3. Timeliness. Unless Provider denies access under this policy, Provider will provide access or send requested copies within 30 days of receipt of the request. If Provider cannot provide the requested records within 30 days, it may extend the response time an additional 30 days if it notifies the Patient or Personal Representative within the initial 30-day period to explain the reason for the delay and the date by which Provider will fulfill the request.

4. Cost for Copies. For records requested by a patient or the Personal Representative, only a reasonable cost-based-fee may be imposed. This reasonable cost-based-fee may include only the cost of: (a) labor for copying the medical records requested by the individual, whether in paper or electronic form; (b) supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (c) postage, when the individual requests that the copy be mailed; and (d) preparation of an explanation or summary of the medical records, if agreed to by the individual.

   The fee may not include costs associated with reviewing the request for access, verifying the request, searching for and retrieving the medical records, storage costs, or other costs not specifically listed in (a)-(d), above. In no event can the fee exceed $0.65 per page. Electronic copies of the medical record, when requested, shall be provided in a readable format and the fee for providing an electronic copy shall not exceed the actual labor cost associated with responding to the request. For electronic copies, instead of calculating a cost-based fee, a flat fee of $6.50 may be charged for the electronic copy.

5. Denial of Access. Under certain limited circumstances permitted under HIPAA, Provider may deny a Patient or Personal Representative's request for access to all or a portion of the PHI requested. A denial can be no broader than necessary to address the reason for the denial, must be based on the specific facts and circumstances surrounding the request and must be approved by the Privacy Officer.

   Unreviewable grounds for denial: (1) the records requested are Psychotherapy Notes; or (2) when the request is for electronic PHI and Provider knows or reasonably suspects that the electronic data is misidentified or mismatched, corrupt due to a technical failure, or erroneous for another reason. (45 CFR 171.201).

Reviewable grounds for denial. The following grounds for denial are determined on an individualized basis by the treating provider: (1) The access requested is reasonably likely to endanger the life or physical safety of the individual or another person, as determined by a licensed health care professional in the exercise of his or her professional judgment.

- Under Conn. Gen. Stat. §20-7c(e), if a provider reasonably determines that the information is detrimental to the physical or mental health of the patient or is likely to cause the patient to harm himself, herself or another, the provider may withhold the information, but this does not apply to information related to psychiatric or psychological problems or conditions.
- Under Conn. Gen. Stat. § 17a-548(b), which applies to requests for records after discharge from an in-patient or out-patient facility for the diagnosis, observation or treatment of a psychiatric disability, Provider may deny access only if there is a substantial risk of life-threatening injury to self or others or severe deterioration in mental state or violation of rights of others.

(2) The requested PHI refers to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; (3) A Patient's Personal Representative makes the request for access and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such Personal Representative is reasonably likely to cause substantial harm to the Patient or another person.

a. *Denials of access based on risk of harm*. Must be made by the Patient's treating provider and that provider must document, with specificity, the reasons for the denial (and those reasons must comply with this policy).

b. *Partial Denials*. If Provider denies the access request in part, it will provide access to the remainder of the requested records.

c. *Written Notice*. For any denial, Provider will provide the requesting Patient or Personal Representative written notice of its denial decision. The written decision must: (i) be provided within 30 day (or 60 days, if Provider complies with the requirements in paragraph 3 above to take advantage of the one-time extension); (ii) be in plain language that the patient can understand; (iii) contain the following three things: (a) the basis for the denial; (b) if the denial reason is reviewable, a statement that the patient has the right to have the denial decision reviewed by responding to the author of the written denial and requesting such a review; and (c) an explanation that the patient can file a complaint with Provider or the Secretary of Health and Human Services.

d. *Denial Because Does Not Maintain.* If Provider denies the request because Provider does not maintain the records and Provider knows where the records are maintained, it will provide that information to the requesting individual.

e. *Review of Denial Decision*. If the individual requests a review, within 10 business days, the Privacy Officer will designate a licensed professional with credentials similar to the

clinician who determined that denial was appropriate to review the matter ("Reviewing Clinician"). The Reviewing Clinician will review all relevant materials and will, within 10 business days of being designated, determine whether the denial decision met the standards set forth in the policy above for a proper denial of access. Provider will implement the decision and promptly provide written notice to the requesting individual of the Reviewing Clinician's decision.

f. *Documentation*. Provider will maintain all documentation relating to the request, the denial and any review for at least six years. A copy of the request for the record must be maintained in the patient's record.

D. Request Amendment of PHI (§164.526)

1. Generally. Provider recognizes that patients have the right to request that Provider amend PHI that is inaccurate or incomplete and to receive a timely response to their requests to amend. Patients must make request to amend in writing.

2. Review of Requests to Amend. The Privacy Officer, in conjunction with appropriate staff is responsible for reviewing all requests to amend and for determining whether the amendment shall be made. The Privacy Officer is responsible for documenting all actions taken in response to requests to amend.

3. Response to Request to Amend. The Privacy Officer responds to a request for an amendment within 60 days of receipt of the request, except that one extension of time to respond which shall not exceed 30 days is permitted as long as Provider notifies the patient in writing of the reasons for the delay.
   a. Denial of Request. The Privacy Officer may deny a request for amendment if he or she determines that the PHI: (i) was not created by Provider, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment; (ii) is not part of the patient's PHI maintained by or on behalf of Provider; or (iii) is accurate and complete. Where a patient's amendment is denied, Provider provides the patient with a timely, written denial setting forth:

      1) the basis for the denial;

      2) the patient's right to submit a written statement disagreeing with the denial and how the patient may file such a statement;

      3) a statement that if the patient does not submit a statement of disagreement, the patient may request that Provider provide the patient's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

      4) a description of the procedures for filing a complaint with Provider or with the Department of Health and Human Services.

The patient may submit a written statement of disagreement, no longer than two (2) pages in length and Provider may prepare a written rebuttal to the statement of disagreement. If such a rebuttal is prepared, Provider provides a copy to the patient.

The Privacy Officer is responsible for ensuring that a copy of the statement of disagreement (or an accurate summary) is appended to the disputed health information in all subsequent disclosures of that information.

b. Grant of Request. If the Privacy Officer determines an amendment is appropriate, the Privacy Officer shall:

1) File the patient's letter in the patient's record and attach copies of amended entries to the letter.

2) Send the patient a letter acknowledging receipt and acceptance of the requested amendment. Copy the appropriate provider or practitioner. File the acknowledgement letter in the patient's health record.

3) Determine if there are individuals (including business associates) to whom the updated information should be sent in addition to those noted on the patient's original request. Obtain an Authorization from the patient, if necessary, and follow the appropriate procedure to fulfill the request.

c. Record Keeping. The Privacy Officer must attach or otherwise link copies of all requests for amendment, denials of requests (if any), statements of disagreement and rebuttals to the relevant portion of the patient's PHI which is disputed.

d. Future Disclosures. In any future disclosures of PHI subject to a request to amend that has been denied, when the patient submits a statement of disagreement, Provider must include the patient's request, Provider's denial and patient's statement of disagreement (or a summary), if any, and Provider's rebuttal, if any, or an accurate summary of those documents. When the patient does not submit a statement of disagreement, Provider must only include the patient's request for amendment and Provider's denial or an accurate summary when patient requests such action.

e. Amendment from Another Entity. If the Privacy Officer is informed by another entity of an amendment to the patient's PHI, Provider shall amend the PHI in accordance with this policy.

E. Accounting of disclosures of PHI (§164.528)

Provider recognizes the right of all patients to receive a written accounting of certain disclosures of their PHI made by Provider as set forth in this Policy and Procedure. Requests for accounting shall be made in writing to the Privacy Officer. The Privacy Officer shall be responsible for receiving and processing requests for accounting. Provider provides an accounting of disclosures for paper records for any period up to six (6) years prior to the date on which the accounting is requested.

Disclosures made for the following purposes are included in Provider's accounting:

- As required by law.
- To public health authorities.
- For reporting abuse, neglect or domestic violence (except to law enforcement officials).
- To health oversight agencies, except that Provider is unable to maintain an accounting of disclosures made regarding federal and state surveys.
- In connection with judicial and administrative proceedings.
- To coroners, medical examiners and funeral directors.
- To organ procurement organizations or similar entities.
- For research, unless there is an Authorization.
- To avert a serious threat to health or safety.
- For law enforcement purposes (except to correctional institutions and in certain custodial situations).
- For workers' compensation.
- For fundraising purposes.
- For specialized government functions except for national security or intelligence.
- Disclosures from an electronic health record to carry out treatment, payment or health care operations.

The Following disclosures are not included in Provider's Accounting Log:

- Disclosures made to carry out treatment, payment and health care operations.
- Disclosures made to the patient requesting the accounting.
- Disclosures incident to a use or disclosure otherwise permitted or required by Provider's policies on uses and disclosures.
- Disclosures pursuant to a written Authorization from the patient.
- Disclosures for Provider's Directory or to persons involved in the patient's care or other disclosures for notification purposes.
- Disclosures for national security or intelligence purposes.
- Disclosures to correctional institutions or law enforcement officials in a custodial situation.
- Disclosures by Provider to its Business Associates.
- Disclosures by Provider's Business Associates. The patient may request an accounting directly from Provider's Business Associates. A list of all Business Associates as well as their contact information will be attached to the accounting response.
- Disclosures as part of a limited data set.

The Privacy Officer shall ensure that all accountings include:

- the date the disclosure was made;
- the name of the entity or person who received the PHI and, if known, the address of such person or entity;
- a brief description of the PHI disclosed;
- a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of the written request for disclosure; and

- a list of all Business Associates and their contact information and an instruction that the patient may contact the business associate directly for an accounting of disclosures by that Business Associate.

If, during the accounting period, Provider has made multiple disclosures to the same person or entity for single purposes, the accounting may be abbreviated to contain:
(a) all of the information required under procedure 7, above, for the initial disclosure; (b) for subsequent disclosures, the frequency, periodicity, or number of disclosures; and (3) the date of the last disclosure during the accounting period.

The Privacy Officer shall respond to all requests for accounting within 60 days after receipt by the Privacy Officer of such request except that the Privacy Officer may extend the time to provide the accounting by no more than an additional 30 days upon providing a written statement to the patient setting forth the reasons for the delay and the day by which Provider will provide the accounting.

Provider does not charge patients for the first accounting in any 12-month period. A reasonable fee may be charged for subsequent requests by the patient within the same 12-month period. The patient shall be given advance notice of any fee and provided an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

V. Administrative requirements (§164.530)

A. Privacy Officer - Provider appoints a Privacy Officer who is responsible for assisting Provider in achieving compliance with all health information privacy laws and regulations. Provider may also appoint a designee to act as the Privacy Officer in the absence of the Privacy Officer. The appointment of the Privacy Officer and designee is made in writing and retained by Provider for six (6) years. The Privacy Officer and designee receive training relevant to their duties.

B. Training - It is the policy of Provider to provide all necessary and appropriate HIPAA training for the members of its workforce to carry out their functions with respect to PHI, including training based on Provider's HIPAA Policies and Procedures. New employees will be trained upon hire and all employees are trained annually. Contingent or temporary personnel and volunteers will receive training on Provider's policies relevant to the work of such individuals prior to beginning work. Provider will keep documentation of all training for at least six (6) years.

C. Safeguards - Provider will ensure that it has appropriate administrative, technical, and physical safeguards in place to protect the confidentiality, integrity and availability of all PHI. Provider takes steps to reasonably safeguard PHI from any intentional, unintentional, or incidental use or disclosure that is in violation of the standards, implementation specifications or other requirements of HIPAA's Privacy and Security Rules. See HIPAA Security Policies.

D. Complaints to Provider/No Retaliation - Provider recognizes that an individual who believes that his or her privacy rights with respect to PHI have been violated has the right to complain to either Provider or the Secretary of Health and Human Services (the "Secretary"). Provider receives complaints from individuals without threat of retaliation, and cooperates with the Secretary, if the Secretary undertakes an investigation or compliance review of Provider's policies, procedures, or practices. Provider will investigate all complaints and will document the results. Provider will not retaliate against any individual for exercising a right to file a complaint or for participating in the investigation process.

E. Sanctions - Provider will take disciplinary action against members of its workforce who fail to comply with Provider's HIPAA Privacy Policies and Procedures. These disciplinary actions are appropriate to the violation(s) and may include termination.

F. Waiver of Rights - Provider will not require individuals to waive their rights to file a complaint with the Department of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

G. Documentation - It is the policy of Provider to maintain records related to compliance with HIPAA for a period of at least six (6) years unless a longer period is required by law.

VI. Breach Notification (§164.400 et. al)

Upon receiving a report of a possible HIPAA violation, Provider shall investigate to determine whether a breach of unsecured PHI has occurred as defined in the regulations. Any impermissible use or disclosure is presumed to be a breach unless the Privacy Officer determines that there is a low probability that the PHI has been compromised based on a risk assessment considering at least the four factors set out in the regulation. The determination of whether a HIPAA violation meets the definition of a breach which requires notification shall be made by the Privacy Officer and shall be documented.

If it is determined that a breach of unsecured PHI has occurred, Provider shall provide written notification to the affected individuals that complies with the Breach Notification Rule by first class mail or by email (if the patient has indicated a preference to receive communications by email) without unreasonable delay, but in no event later than 60 days after the breach is discovered. In urgent situations where possible misuse of unsecured information is a concern, notice may be provided to individuals by phone in addition to the written notice.

If a breach involves ten or more patients whose contact information is out of date, a notice of breach will be posted on Provider's website.

In the event of a breach involving more than 500 patients, notice will be provided to the Secretary contemporaneously with the notifications to the individuals and in the manner specified on the Department of Health and Human Services website. For breaches involving more than 500 patients of a State or jurisdiction, notice will also be provided to a prominent media outlet in the jurisdiction within the same timeframe as the individual notifications (without unreasonable delay and in no case later than 60 days after discovery of the breach). Notification to the media will include the same information provided to the individuals.

The written notification shall include: (1) A brief description of what happened, including the date of the breach and date of discovery of the breach, if known; (2) A description of the type of unsecured PHI that was involved in the breach (without referencing specific information); (3) Any steps individuals should take to protect themselves from potential harm resulting from the breach; (4) A brief description of what Provider is doing to investigate the breach, to mitigate harm to the individuals and to protect against further breaches; and (5) Contact procedures for individuals to ask questions or learn additional information.

No later than 60 days after the end of each calendar year, the Privacy Officer, or his/her designee, shall submit an annual report to the Secretary of any breaches of unsecured PHI which

occurred during the calendar year at https://ocrnotifications.hhs.gov. A copy of such filing shall be maintained for a period of six (6) years.

VII. Behavioral Health Records (state law)

Provider adheres to Connecticut state law, which is more stringent than the federal Privacy Regulations with respect to behavioral health records. This policy is based on the rules specific to professional counselors (Conn. Gen. Stat. §52-146s).

A privilege attaches to an individual's communications with a professional counselor. "Communications" means all oral and written communications and records thereof relating to the diagnosis and treatment of a person between such person and a professional counselor or between a member of such person's family and a professional counselor.

Provider will not use or disclose its communications and records unless the patient or parent, legal guardian or authorized representative waive the privilege through an Authorization. If more than one person in a family is receiving therapy, each such family member must agree to waive the privilege and authorize the use or disclosure. In the absence of such a waiver from each such family member, Provider shall not disclose communications with any family member.

An Authorization is not required when: (1) mandated by any other provision of the general statutes; (2) Provider believes in good faith that the failure to disclose such communications presents a clear and present danger to the health or safety of any individual; or (3) Provider makes a claim for collection of fees for services rendered, after making a written demand directly to the individual at least thirty days prior to such disclosure. Such disclosure may include only name, address, and services information.

When confidential behavioral health records are disclosed, they shall be accompanied by the following statement:

"The confidentiality of this record is required under Chapter 899 of the Connecticut General Statutes. This material shall not be transmitted to anyone without written consent or other Authorization as provided in the aforementioned Statutes." In cases where the disclosure is made verbally, the person disclosing the information shall inform the recipient that such information is governed by the provisions of Sections 52-146c to 52-146f, inclusive.